

Il futuro regolamento EU sui dati personali e la valenza 'politica'
del caso Google: ricordare e dimenticare nella digital economy

Original

Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy / Mantelero, Alessandro - In: Il diritto all'oblio su Internet dopo la sentenza Google Spain / Giorgio Resta e Vincenzo Zeno-Zencovich. - STAMPA. - Roma : Roma Tre-Press, 2015. - ISBN 978-88-97524-24-3. - pp. 125-146

Availability:

This version is available at: 11583/2601158 since: 2016-07-28T17:41:45Z

Publisher:

Roma Tre-Press

Published

DOI:

Terms of use:

openAccess

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

Collana “Consumatori e Mercato”

3

IL DIRITTO ALL’OBLIO SU INTERNET DOPO LA SENTENZA GOOGLE SPAIN

a cura di **Giorgio Resta** e **Vincenzo Zeno-Zencovich**



Roma TrE-Press

2015

Questo volume è stato realizzato nel quadro di una ricerca coordinata dalla Fondazione “Centro di iniziativa giuridica Piero Calamandrei” sui temi del diritto all’anonimato e all’oblio su Internet, e la cui pubblicazione è stata finanziata dal Ministero per i Beni Culturali.

PRESENTAZIONE DELLA COLLANA “CONSUMATORI E MERCATO”

DIRETTORE: VINCENZO ZENO-ZENCOVICH

COMITATO SCIENTIFICO: GUIDO ALPA, MARCELLO CLARICH, ALBERTO MUSSO

La Collana “Consumatori e mercato”, per le Edizioni Universitarie di Roma Tre all’interno del progetto di Ateneo Roma TrE-Press, intende essere una piattaforma editoriale multilingue, avente ad oggetto studi attinenti alla tutela dei consumatori e alla regolazione del mercato. L’intento è di stimolare un proficuo scambio scientifico attraverso una diretta partecipazione di studiosi appartenenti a diverse discipline, tradizioni e generazioni.

Il dialogo multidisciplinare e multiculturale diviene infatti una componente indefettibile nell’ambito di una materia caratterizzata da un assetto disciplinare ormai maturo tanto nelle prassi applicative del mercato quanto nel diritto vivente. L’attenzione viene in particolare rivolta al contesto del diritto europeo, matrice delle scelte legislative e regolamentari degli ordinamenti interni, e allo svolgimento dell’analisi su piani differenti (per estrazione scientifica e punti di osservazione) che diano conto della complessità ordinamentale attuale.

The “Consumer and market” series edited by Edizioni Universitarie di Roma Tre for the Roma TrE-Press project, aims at being a multilingual editorial project, which shall focus on consumer protection and market regulation studies. The series’ core mission is the promotion of a fruitful scientific exchange amongst scholars from diverse legal systems, traditions and generations. This multidisciplinary and multicultural exchange has in fact become fundamental for a mature legal framework, from both the market practice and the law in action standpoints. A particular focus will be given on European law, where one can find the roots of the legislation and regulation in the domestic legal systems, and on the analysis of different levels, in line with the current complexity of this legal sector.

Elenco e qualifiche degli autori

Giandonato CAGGIANO, *ordinario di diritto dell'Unione Europea nell'Università Roma Tre*
Cosimo COMELLA, *dirigente presso il Garante per la protezione dei dati personali*
Virgilio D'ANTONIO, *associato di diritto privato comparato nell'Università di Salerno*
Giusella FINOCCHIARO, *ordinario di diritto privato nell'Università di Bologna*
Roberto FLOR, *ricercatore di diritto penale nell'Università di Verona*
Tommaso Edoardo FROSINI, *ordinario di diritto pubblico comparato nell'Istituto Universitario Suor Orsola Benincasa di Napoli*
Alessandro MANTELERO, *aggregato di diritto privato nel Politecnico di Torino*
Paola PIRODDI, *associato di diritto dell'Unione Europea nell'Università di Cagliari*
Franco PIZZETTI, *ordinario di diritto costituzionale nell'Università di Torino*
Oreste POLLICINO, *associato di diritto pubblico comparato nell'Università Bocconi di Milano*
Giovanni Maria RICCIO, *associato di diritto privato comparato nell'Università di Salerno*
Giovanni SARTOR, *ordinario di filosofia del diritto nell'Università di Bologna*
Salvatore SICA, *ordinario di diritto privato comparato nell'Università di Salerno*
Mario VIOLA DE AZEVEDO CUNHA, *associato di diritto privato nell'Università statale di Rio de Janeiro*

Coordinamento editoriale:

Gruppo di Lavoro *RomaTrE-Press*

Elaborazione grafica della copertina: Mosquito mosquitoroma.it

Edizioni: RomaTrE-Press ©

Roma, aprile 2015

ISBN: 978-88-97524-24-3

<http://romatrepress.uniroma3.it>

Quest'opera è assoggettata alla disciplina *Creative Commons attribution 4.0 International License* (CC BY-NC-ND 4.0) che impone l'attribuzione della paternità dell'opera, proibisce di alterarla, trasformarla o usarla per produrre un'altra opera, e ne esclude l'uso per ricavarne un profitto commerciale.



Indice

TOMMASO EDOARDO FROSINI, <i>Google e il diritto all'oblio preso sul serio</i>	1
ORESTE POLLICINO, <i>Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain</i>	7
GIUSELLA FINOCCHIARO, <i>Il diritto all'oblio nel quadro dei diritti della personalità</i>	29
GIANDONATO CAGGIANO, <i>L'interpretazione del criterio di collegamento del "contesto delle attività di stabilimento" dei responsabili del trattamento dei dati personali</i>	43
PAOLA PIRODDI, <i>Profili internazionalprivatistici della responsabilità del gestore di un motore di ricerca per il trattamento di dati personali</i>	63
GIOVANNI SARTOR, MARIO VIOLA DE AZEVEDO CUNHA, <i>Il caso Google e i rapporti regolatori USA/EU</i>	99
ALESSANDRO MANTELERO, <i>Il futuro regolamento EU sui dati personali ed il dilemma del caso Google: ricordare e dimenticare nella digital economy</i>	125
SALVATORE SICA, VIRGILIO D'ANTONIO, <i>La procedura di de-indicizzazione</i>	147
COSIMO COMELLA, <i>Indici, sommari, ricerche e aspetti tecnici della de-indicizzazione</i>	177
GIOVANNI MARIA RICCIO, <i>Diritto all'oblio e responsabilità dei motori di ricerca</i>	199
ROBERTO FLOR, <i>Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?</i>	223
FRANCO PIZZETTI, <i>Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il "velo di Maya"</i>	255
APPENDICE	
1. <i>Corte di Giustizia dell'Unione Europea (Grande Sezione) - 13 maggio 2014 Sentenza nella causa C-131/12</i>	283
2. <i>Conclusioni dell'Avvocato Generale Niilo Jääskinen nella causa C-131/12</i>	314

Tommaso Edoardo Frosini

Google e il diritto all'oblio preso sul serio

1. Lo studioso di diritto della comunicazione non può non guardare con grande attenzione alla sentenza della Corte di Giustizia dell'Unione Europea (causa C-131/12) del 13 maggio 2014, nota come *Google Spain*. La decisione giurisprudenziale è di sicura importanza e, piaccia oppure no, segna uno spartiacque nel *digital right to privacy*. Perché impone ai motori di ricerca, a partire da *Google*, l'applicazione della normativa europea sulla protezione dei dati personali, valorizzando oltremodo il cd. Diritto all'oblio.

Certo, non c'è solo l'oblio nella sentenza; ci sono, piuttosto, numerosi spunti di riflessioni, che sono oggetto di commento nei contributi che appaiono in questo fascicolo. E quindi: *a)* l'applicazione delle norme europee nei confronti dei gestori dei motori di ricerca, che non hanno sede in Europa ma che abbiano una stabile organizzazione in un Paese della UE; *b)* l'attività tipica svolta da un motore di ricerca, che è da qualificarsi come «trattamento dei dati personali», e pertanto il gestore deve rispettare la normativa europea sulla protezione dei dati; *c)* nel rispetto della normativa europea, corre l'obbligo al gestore del motore di ricerca – in presenza di determinate condizioni – di rimuovere dall'elenco dei risultati di una ricerca sul nome di un soggetto quei *link* verso pagine *web* che contengono informazioni relative al soggetto stesso; *d)* il soggetto interessato, sulla base degli artt. 7 e 8 della Carta dei diritti fondamentali della UE, può chiedere direttamente al motore di ricerca che l'informazione relativa alla sua persona non venga più messa a disposizione degli utenti della rete, ovvero venga cancellata, e così facendo esercita il suo diritto all'oblio; *e)* vengono infine individuati i criteri attraverso i quali svolgere il giudizio di bilanciamento tra gli interessi coinvolti. Sul punto, conviene citare un passo della sentenza: «*i diritti fondamentali di cui sopra [quelli protetti dagli artt. 7 e 8 della Carta] prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona*».

Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari,

come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi ». Periodare affannato ma che fa risaltare la complessità della questione. Che si può sintetizzare nel riconoscimento del prevalere dei diritti fondamentali della persona rispetto al diritto all'informazione e ai diritti economici delle imprese.

2. Quindi non c'è solo l'oblio nella sentenza; ma è senz'altro questo diritto che suscita la maggiore attrattività dell'esegesi giuridica. Nuovo diritto, che si declina come una pretesa a riappropriarsi della propria storia personale, e quindi come una sorta di diritto all'autodeterminazione informativa, ovvero il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati che lo riguardano. Si tratta dell'applicazione teorica della dottrina del diritto di libertà informatica, enunciata a inizi anni Ottanta, nel suo duplice volto: negativa e positiva. La libertà informatica *negativa*, esprime il diritto di non rendere di dominio pubblico certe informazioni di carattere personale, privato, riservato; la libertà informatica *positiva*, invece, esprime la facoltà di esercitare un diritto di controllo sui dati concernenti la propria persona che sono fuoriusciti dalla cerchia della *privacy* per essere divenuti elementi di *input* di un programma elettronico; e dunque libertà informatica positiva, o diritto soggettivo riconosciuto, di conoscere, di correggere, di togliere o di aggiungere dati in una scheda personale elettronica. Ecco che così il diritto di libertà informatica assume una nuova forma del tradizionale diritto di libertà personale, come diritto di controllare le informazioni sulla propria persona, come diritto dello *habeas data* (sul punto, rinvio al mio scritto: *Il diritto all'oblio e la libertà informatica*, in *Dir. Inf.*, 2012, 910 ss.). Certo, va altresì detto che il diritto all'oblio trae la sua forza costituzionale nella dignità umana, valore non negoziabile del costituzionalismo contemporaneo.

Con specifico riguardo alla sentenza della CGUE, c'è da rilevare una sorta di confusione nell'interpretazione del trattamento dei dati personali, perché una cosa è il trattamento illecito un'altra è quello lecito ma soggetto alla richiesta di oblio da parte dell'interessato.

Il punto è esattamente colto da Oreste Pollicino nel suo contributo *infra* pubblicato. Vale citare, a proposito, la giurisprudenza di legittimità italiana, che si è più volte pronunciata in tema di diritto all'oblio (da ultimo, Cass., n. 5525 del 2012 e n. 16111 del 2013). Riconoscendogli una chirurgica precisione nell'applicazione di questo diritto, specie nella parte in cui ha previsto non la cancellazione della notizia ma piuttosto la con-

testualizzazione', e quindi l'aggiornamento, da parte del titolare del sito, della notizia che riguarda direttamente il soggetto. Perché una notizia non aggiornata non è una notizia vera. È questo un aspetto assai significativo e sul quale occorre riflettere: la notizia apparsa sul *web* non dura, al pari delle notizie sulla carta stampata, come la rosa di Ronsard, *l'espace d'un matin*, ma piuttosto assume forma durevole e incancellabile; chiunque la può leggere e rileggere, ovunque si trova nel mondo, e può 'utilizzarla' come fonte di informazione. Ma la notizia non è un dato astratto alla *mercé* di tutti, perché riguarda la persona e la sua immagine in un dato momento storico; i dati personali, vale la pena ricordarlo, costituiscono una parte della espressione della personalità dell'individuo. E allora, deve essere consentito alla persona, a tutela della sua identità, di esercitare il proprio diritto di libertà informatica, che consiste nel potere disporre dei propri dati, ovvero delle notizie che lo riguardano, e quindi chiedere per ottenere sia il diritto all'*oblio* su ciò che non è più parte della sua identità personale, sia il diritto alla *contestualizzazione* del dato, e quindi della notizia, perché «una verità non aggiornata non è una verità».

Va comunque detto, che nel caso *Google Spain* la notizia non richiedeva un aggiornamento, e unica ragione della sua illegittimità era quella di essere presente in rete troppo a lungo rispetto a quanto sarebbe ragionevole che fosse, tenendo conto del diritto del soggetto coinvolto a non essere ricordato per qualcosa che non sarebbe più di nessuna rilevanza sociale.

3. C'è inoltre una questione che emerge nella vicenda *Google Spain*: ed è quello a conferma dell'attivismo giurisdizionale in tema di Internet e aspetti regolativi dello stesso. Sono i giudici, nazionali ed europei, che stanno mostrando attenzione e sensibilità allo sviluppo del diritto nella società tecnologica, atteggiandosi come in ambiente di *common law*. Prima della sentenza *Google Spain*, si può ricordare la sentenza della Corte EDU del 16 luglio 2013 (*Węgrzynowski e Smolczewski vs. Polonia*), con la quale si è affermato che dalla CEDU non è possibile ricavare il diritto di un soggetto alla rimozione dal sito internet di un giornale di un articolo lesivo della propria reputazione, nemmeno dopo l'accertamento definitivo del carattere illecito dello stesso. E si può altresì citare anche una sorta di *self-restrain*, laddove il giudice di Strasburgo scrive: «non è compito dell'autorità giudiziaria riscrivere la storia, ordinando di far scomparire dal pubblico dominio tutte le tracce di una pubblicazione che pure è stata ritenuta, da sentenze definitive, costituire una ingiustificata violazione della reputazione di un individuo». Dopo la sentenza *Google Spain*, si può invece ricordare, come ha fatto Pollicino nel saggio *infra*, la pronuncia della Corte suprema

dello stato canadese di *British Columbia*, che aveva a che fare con un caso di concorrenza sleale nel campo della produzione di prodotti *high tech*, ha testualmente concluso che «*an interim injunction should be granted compelling Google to block the defendants' websites from Google's search results worldwide*». Infine: va qui dato atto a *Google* di avere intrapreso un'azione a rispetto della sentenza della CGUE, consistente, per ora, nel rendere disponibile una modulistica per la domanda di rimozione dei dati, che deve essere comunque sottoposta a valutazione da parte dell'azienda, per «bilanciare i diritti sulla *privacy* della persona con il diritto di tutti di conoscere e distribuire le informazioni». Certo, non può non lasciare quantomeno perplessi questa funzione paracostituzionale attribuita a un'azienda privata, peraltro riconosciutagli dal giudice della Corte europea.

Ma *Google* ha fatto anche altro: ha nominato un comitato consultivo sul diritto all'oblio composto da personalità internazionali, che ha aperto una piattaforma *on line* (www.google.com/advisorycouncil/) chiedendo pareri su «come dovrebbe essere bilanciato il diritto all'oblio di una persona con il diritto del pubblico di sapere?», e convocando un primo *meeting* a Madrid e un secondo a Roma nel settembre 2014.

Di recente, in un saggio apparso su *Percorsi costituzionali* (n.1, 2014), ho provato ad argomentare su *Internet come ordinamento giuridico*. L'elaborazione di una teoria di internet, ovvero il *cyberspace*, come ordinamento giuridico autonomo, muove dall'assunto che «*cyberspace is a distinct place for purposes of legal analysis by recognizing a legally significant border between cyberspace and the real world*». Ancora, il *cyberspace* diventa «*an important forum for the development of new connections between individuals and mechanism of self-governance*». Un diritto spontaneo, quindi. Un diritto pari a quello della *lex mercatoria*, con la quale si regolavano i rapporti commerciali nel medioevo. Una *lex informatica*, dunque; che può avvalersi di una *co-regulation*, in cui le leggi statali si verrebbero a integrare con una politica di *self-regulation* da parte degli utenti di internet.

Una sorta di applicazione del principio di sussidiarietà, in cui la *co-regulation* dello Stato può venire in sussidio alla *self-regulation* degli utenti, quando questi la evocano ovvero quando la necessitano.

Un'ultima considerazione, infine, di politica del diritto. Nel Ventunesimo secolo l'antiliberalismo si misura su Internet. Infatti, è diventato questo il luogo dove si manifestano le intolleranze, si esercitano le censure e si imbavaglia il dissenso *online*.

Muri virtuali vengono eretti al posto di quelli di pietra: ci sono Paesi che hanno costruito barriere elettroniche per evitare l'accesso a parte della

rete globale, e lo hanno fatto cancellando parole, nomi e frasi chiave dei motori di ricerca, oppure violando la *privacy* dei cittadini. Una nuova cortina d'informazione sta scendendo su una parte del mondo, dove i video e i blog sono ormai i *samizdat* dei giorni nostri. Questo però conferma la vocazione liberale di Internet, e la paura che di questa libertà globale mostrano di avere Paesi intolleranti alla tecnologia, perché la vivono come una minaccia al loro potere assoluto. E allora, il motto della nuova 'rivoluzione' costituzionale è: *Liberté, Egalité, Internet*.

Oreste Pollicino

Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della carta di Nizza nel reasoning di Google Spain

SOMMARIO: 1 Introduzione - 2. Il ruolo degli artt. 7 ed 8 della Carta di Nizza nella giurisprudenza precedente della Corte di giustizia... - 3. ...Ed il nuovo (ingigantito) ruolo giocato da questi ultimi nel *reasoning* di Google Spain - 4 Considerazioni finali

1. Introduzione

«La costellazione particolarmente complessa e difficile di diritti fondamentali che questo caso presenta, osta alla possibilità di rafforzare la posizione giuridica della persona interessata ai sensi della direttiva riconoscendole un diritto all'oblio. Ciò vorrebbe dire sacrificare diritti primari come la libertà di espressione e di informazione. Inoltre, inviterei la Corte a non concludere che questi interessi concorrenti possono essere ponderati in modo soddisfacente in situazioni individuali sulla base di una valutazione caso per caso, lasciando la decisione ai fornitori di servizi di motore di ricerca su Internet»¹.

Questo è quanto l'Avvocato generale Jääskinen, nelle sue conclusioni, proponeva alla Corte di Lussemburgo in merito al bilanciamento tra i diritti coinvolti, nella sua bella immagine, in una «costellazione particolarmente complessa » alla base del caso c.d. *Google Spain*². Un caso ormai

¹ Conclusioni dell'Avvocato Generale Jääskinen presentate il 25 giugno 2013, C-131/12.

² Il tema sul quale la Corte di giustizia è stata chiamata, con un rinvio sollevato nel 2012, dall'Audiencia Nacional spagnola, a pronunciarsi in via pregiudiziale riguarda il rapporto tra la disciplina affidata alla Direttiva 95/46/CE, che costituisce la normativa di riferimento tuttora vigente in materia di dati personali a livello dell'Unione europea, e gli Internet service provider che gestiscono un motore di ricerca, ed in particolare Google. Nel caso che ha originato il rinvio pregiudiziale, l'Agencia Española de Protección de

fin troppo conosciuto, le cui innumerevoli implicazioni, non solo strettamente giuridiche, sono al centro di questo Volume.

Si fa fatica a ricordare dei precedenti a Lussemburgo in cui la Corte di giustizia abbia raggiunto non soltanto una conclusione opposta a quella caldeggiata dall'Avvocato generale, ma anche un percorso argomentativo radicalmente differente da quello proposto da quest'ultimo. Sarebbe sufficiente riformulare, *a contrario*, il passaggio dell'Avvocato generale citato in apertura che, a ben vedere, si compone di due elementi portanti, per identificare, scontando, ovviamente, un inevitabile tasso di semplificazione ed approssimazione, i due (uguali e contrari) punti cardinali emergenti dall'operazione di (non) bilanciamento operata dalla Corte di giustizia. Infatti, con riguardo al primo elemento portante che sembra caratterizzare detto passaggio, i giudici di Lussemburgo, esattamente (e letteralmente) al contrario di quanto si legge nelle riflessioni dell'Avvocato generale prima richiamate, rafforzano decisamente la posizione giuridica della persona interessata (ai sensi della direttiva 95/46) riconoscendole, in sostanza, e forse tecnicamente, quel diritto all'oblio³ che l'Avvocato generale invece negava, come si è appena letto, fosse possibile identificare alla luce dell'esistente *acquis comunitario*. E lo fanno, sacrificando, come si vedrà

Datos, l'autorità iberica per la protezione dei dati personali, aveva ordinato a Google di rimuovere dai risultati generati attraverso il suo motore di ricerca i collegamenti ad alcune notizie relative ad un pignoramento subito dal sign. Costeja González, ricorrente davanti alla stessa Agencia, considerate ormai prive di rilevanza Google rifiutava di ottemperare al provvedimento allegando la sua presunta estraneità alla disciplina europea sui dati personali (e, di conseguenza, a quella spagnola) e rilevando come un intervento come quello imposto dall'Autorità potesse configurare un'indebita compromissione della libertà di espressione dei gestori di siti Internet. Piuttosto, ad avviso del motore di ricerca, solo un intervento sui siti soggetti a indicizzazione avrebbe garantito soddisfazione alla pretesa di ritorno all'anonimato da parte degli interessati. L'Audiencia Nacional, investita dell'appello contro il provvedimento dell'AEPD, sollevava pertanto un rinvio pregiudiziale, formulando tre complessi quesiti volti a verificare, in sostanza, l'applicabilità a un provider come Google della Direttiva 95/46 e la possibilità di garantire l'*enforcement* del diritto all'oblio da parte dei soggetti cui i dati personali si riferiscono.

³ Per alcune osservazioni critiche, si veda T.E. FROSINI, *Diritto all'oblio e Internet* e F. PIZZETTI, *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, entrambi in www.federalismi.it, focus comunicazioni, nuove tecnologie e media, 10 giugno 2014. Si vedano anche i commenti a caldo di C. BLENGINO, *La Corte di giustizia e i motori di ricerca: una sentenza sbagliata*, in www.medialaws.eu, 19/05/2014 [consultato 30/09/2014]; G. CORRIAS LUCENTE, *Ancora su Google e il diritto all'oblio*, in www.medialaws.eu, 24/06/2014 [consultato 30/09/2014]; M. BASSINI, *Google e diritto all'oblio: cosa accade ora?*, in www.voxdiritti.it [consultato 30/09/2014]; ID., *Il diritto all'oblio ai tempi di Internet: la Corte di giustizia sui motori di ricerca*, in *Quad. cost.*, in corso di pubblicazione.

più avanti, proprio quelle libertà di informazione e di espressione che lo stesso Avvocato generale definisce, sempre nello stesso passaggio, 'diritti primari'.

Con riferimento al secondo elemento portante dell'*incipit* con cui si è aperto questo contributo, non sembra essere così lontano dal vero affermare, salvo poi integrare e precisare nel prosieguo⁴, che nuovamente, esattamente e (letteralmente) all'opposto di quanto proposto dallo stesso Jääskinen, i giudici concludono, in sostanza, e con implicazioni non di poco conto, che il bilanciamento tra i diritti confliggenti prima evocati (da una parte diritto all'oblio, dall'altra libertà di informazione e espressione) può essere operato in modo soddisfacente in situazioni individuali sulla base di una valutazione caso per caso, lasciando, di fatto, contrariamente a quanto caldamente consigliato dall'Avvocato generale, la decisione ai fornitori di servizi di motore di ricerca su Internet.

Sarebbe, forse, interessante esplorare le ragioni alla base di un disostamento così netto, da parte della Corte di Lussemburgo, dalla posizione adottata dall'Avvocato generale, ma un'indagine di questo tipo andrebbe ben al di là dei confini tematici che mi sono stati assegnati. Per questa ragione, le differenze (evidenti, quasi abissali in vero) tra natura degli argomenti ed esito dei bilanciamenti caratterizzanti i *reasoning*, rispettivamente, di Jääskinen da una parte e della Grande Camera dall'altra, saranno prese in considerazione esclusivamente nella misura in cui si rivelano utili al tentativo di fornire una risposta adeguata all'interrogativo centrale alla base di questo contributo. Vale a dire: che ruolo hanno giocato i diritti al rispetto della vita privata ed al trattamento dei propri dati personali, previsti, rispettivamente, dagli artt. 7⁵ ed 8⁶ della Carta dei diritti fondamentali dell'Unione europea, nell'emersione, sempre più prepotente, alla luce della pronuncia *Google Spain*, ma anche della decisione della stessa Corte di Lussemburgo⁷, di poco precedente, che ha annullato la direttiva

⁴ Si rimanda in proposito agli scritti di Giovanni Maria Riccio e Roberto Flor in questo volume.

⁵ Ai sensi dell'art. 7: «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

⁶ Ai sensi dell'art. 8: 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente ».

⁷ Corte di giustizia dell'Unione europea, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland, Seitlinger and Others*, in *Dir.Inf.* 2014, 851.

in materia di *data retention*, di un vero e proprio *digital right to privacy*?

Al fine di provare a rispondere al quesito appena enunciato, il contributo, dopo aver fatto un sintetico riferimento al portato normativo che caratterizza gli artt. 7 ed 8 della Carta ed al ruolo giocato da tali previsioni in una prima fase della giurisprudenza rilevante della Corte di Lussemburgo, si concentrerà sull'approfondimento del come e del perché tale ruolo si sia ingigantito nella decisione oggetto di indagine. Le riflessioni finali tenteranno di contestualizzare le risultanze emerse dall'indagine all'interno dell'assai cangiante rapporto (*à trois*) tra tutela dei diritti fondamentali, dimensione digitale ed elemento territoriale.

2. Il ruolo degli artt. 7 ed 8 della carta di Nizza nella giurisprudenza precedente della Corte di giustizia...

Delle due previsioni normative oggetto di indagine in questa sede, non ci sono dubbi che è l'art. 8 della Carta ad avere un maggiore portato innovativo⁸. Nonostante il tentativo da parte delle Spiegazioni allegate alla Carta di restringerne la portata ad una mera riproposizione dell'*acquis* esistente⁹, in realtà, il margine di innovazione dell'art. 8 è piuttosto significativo. E non consiste soltanto nel 'costituzionalizzare' il diritto alla protezione dei dati personali, ma anche, e forse specialmente, nell'emanipare definitivamente quest'ultimo da quella connessione alla dimensione economica propria del consolidamento del mercato interno che invece caratterizzava, almeno *ab origine*, il portato normativo della direttiva

⁸ Il che è peraltro confermato dalle Spiegazioni all'articolo 7 in cui si legge che «I diritti di cui all'articolo 7 corrispondono a quelli garantiti dall'articolo 8 della CEDU. Per tener conto dell'evoluzione tecnica, il termine comunicazioni è stato sostituito a 'corrispondenza'. Conformemente all'articolo 52, paragrafo 3, il significato e la portata di questi diritti sono identici a quelli del corrispondente articolo della CEDU. Le limitazioni che vi possono legittimamente essere apportate sono pertanto quelle autorizzate ai sensi del suddetto articolo 8.

⁹ Ai sensi delle Spiegazioni: «Questo articolo si fonda sull'articolo 286 del trattato che istituisce la Comunità europea, sulla direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GU L 281 del 23.11.95), nonché sull'articolo 8 della CEDU e sulla convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del 28 gennaio 1981, ratificata da tutti gli Stati membri. Il diritto alla protezione dei dati personali si esercita alle condizioni previste dalla suddetta direttiva e può essere limitato alle condizioni previste dall'articolo 53 della Carta».

95/46¹⁰. È vero, a partire dall'entrata in vigore del Trattato di Lisbona che, come è notissimo, è coinciso con l'attribuzione di un carattere vincolante alla Carta di Nizza, tale tutela para-costituzionale del diritto alla protezione dei dati personali è condivisa anche dal primo comma dell'art. 16 TFUE¹¹, ma non può non essere sottolineato come a emergere quale pioniere in questo senso, sia stato, sin dal 2001, proprio l'art. 8 della Carta che, tra l'altro, 'costituzionalizza' anche, unica tra le autorità indipendenti, il ruolo del Garante per la protezione dei dati personali.

Nella giurisprudenza precedente al terribile 'uno/due' di Lussemburgo costituito dalle decisioni in tema di *data retention* e diritto all'oblio, può identificarsi, con la necessaria semplificazione dovuta al rispetto delle esigenze di sintesi in relazione ad un panorama giurisprudenziale logicamente e cronologicamente precedente rispetto a quello che costituisce oggetto privilegiato di questo contributo, una duplice caratterizzazione nella giurisprudenza rilevante. Da una parte, un approccio per così dire omnicomprensivo dei giudici comunitari alla protezione della *privacy*, volto a fare un riferimento spesso cumulativo agli artt. 7 e 8 della Carta senza fare emergere con chiarezza l'autonomia concettuale del diritto alla protezione dei dati personali rispetto al classico diritto al rispetto della vita privata. Dall'altra parte, quando è emerso il tema delle limitazioni consentite ai diritti previsti dagli artt. 7 e 8, ed in particolare, dunque, con riferimento all'applicazione dell'art. 52¹² della Carta, i giudici comunitari non avevano mai distinto, fino alle decisioni di questi ultimi mesi, i due profili presenti nella previsione ora richiamata: da un lato, quello relativo all'applicazione del principio di proporzionalità, dall'altro lato, quello riguardante la vio-

¹⁰ Come *inter alia*, in primo luogo, dalla circostanza, di per sé cruciale, che la base giuridica identificata per l'adozione della direttiva è stata l'ex art. 100 A, introdotto con l'Atto Unico Europeo e poi divenuto art 95 TCE, che è per l'appunto il fondamento di tutti gli atti dell'UE che hanno per oggetto l'armonizzazione delle misure nazionali relativi all'instaurazione ed al funzionamento del mercato interno. In secondo luogo da quanto si legge nel terzo considerando della direttiva, ai sensi del quale, «l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 7 A del Trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona».

¹¹ Ai sensi del quale ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

¹² Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

lazione dei contenuti essenziali dei diritti in gioco.

Con riguardo, in particolare, alla prima delle due attitudini appena descritte, un esempio abbastanza emblematico può essere rintracciato nella sentenza *Shelcke* del 2010¹³, in cui i giudici comunitari testualmente affermano che «si deve ritenere, da un lato, che il rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli artt. 7 e 8 della Carta, sia riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile...e, dall'altro, che le limitazioni che possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispondano a quelle tollerate nell'ambito dell'art. 8 della CEDU (par. 52)». A ben vedere, lo stesso riferimento, nella decisione per ultimo richiamata, all'art. 8 della CEDU fa emergere come il diritto alla protezione dati sia considerato semplicemente quale una appendice accessoria rispetto al diritto al rispetto alla vita privata previsto dall'art. 7 della Carta, ed in particolare, sia inteso quale diritto alla predeterminazione informativa che non può non rievocare l'*Informationelle Selbstbestimmung* di matrice tedesca¹⁴. Il che, però, non sembra corrispondere alle intenzioni dei redattori della Carta. Mentre, infatti, come 8, si è voluto emancipare, almeno in alcuni casi, il trattamento dei dati dal consenso iniziale dell'avente diritto¹⁵. Come infatti è stato acutamente rilevato, l'art. 8 riflette un *acquis* comunitario in materia di protezione dati che «*looks beyond consent only and create a system of checks and balances which ensures lawful processing also without asking the consent of the person involved*»¹⁶.

¹³ Corte di giustizia, 9 novembre 2010, C-92/09 e C-93/09, *Volker and Markus Schelke*, par. 52. Altro passaggio che testimonia l'attitudine della Corte di giustizia ad una piuttosto indifferenziata lettura degli artt. 7 ed 8 è quello in cui, nella pronuncia appena richiamata si legge espressamente che gli articoli 7 e 8 della Carta sono strettamente legati al punto da poter essere considerati come integranti un «diritto alla vita privata» con riguardo al trattamento dei dati personali (par. 52).

¹⁴ Come *BVerfG* nel caso *Volkszählung (Microcensus)*.

¹⁵ Come è chiaro dal riferimento che le Spiegazioni fanno (anche) alla Convenzione n. 108 del 1981 del Consiglio d'Europa che non fa del consenso dell'avente diritto un principio fondante.

¹⁶ H. KRANENBORG, *Article 8*, in S. PEERS, T. HARVEY, J. KENNER, A. WARD (a cura di), *The EU Charter of Fundamental Rights: a Commentary*, Oxford-Portland, Oregon, Hart Publishing, 2014, pp. 224 ss., 229.

3. ...ed il nuovo (ingigantito) ruolo giocato da questi ultimi nel reasoning di *Google Spain*

Ebbene, come anticipato, prima ancora che in *Google Spain*, è nella decisione di poco precedente che annulla la direttiva in materia di *data retention* che i giudici comunitari innovano rispetto alla giurisprudenza rilevante. Da una parte, per la prima volta, sembrano infatti più inclini a considerare la rilevanza autonoma dei due diritti previsti dagli artt. 7 e 8 della Carta¹⁷, dall'altra, fanno emergere una distinzione piuttosto netta tra, per un verso, il profilo (non riscontrato nel caso di specie) di violazione, da parte della direttiva, del contenuto essenziale di tali diritti¹⁸ e, per altro verso, quello relativo all'accertamento della proporzionalità delle misure identificate dalla stessa direttiva per realizzare gli obiettivi previsti di tutela dell'ordine pubblico e lotta contro il terrorismo. Misure, quest'ultime, invece considerate dalla Corte di Lussemburgo eccessivamente intrusive nei confronti dei diritti al rispetto alla vita privata ed alla protezione dei dati personali.

Il percorso avviato in occasione della sentenza in tema di *data retention* e tendente alla identificazione di un *digital (Internet based) right to data protection* che, a dettato normativo invariato, i giudici comunitari fanno emergere da una lettura estensiva, o meglio manipolativa, assiologicamente

¹⁷ Anche se emerge ancora la tendenza ad una tutela indifferenziata, laddove, nella sentenza *Google Spain*, al par. 53, testualmente si dice che occorre ricordare che la tutela dei dati personali, risultante dall'obbligo esplicito previsto all'articolo 8, paragrafo 1, della Carta, riveste un'importanza particolare per il diritto al rispetto della vita privata sancito dall'articolo 7 della stessa.

¹⁸ Chiarissimi, in questo senso, i parr. 39 e 40 della pronuncia, in cui si legge che «per quanto riguarda il contenuto essenziale del diritto fondamentale al rispetto della vita privata e degli altri diritti sanciti all'articolo 7 della Carta, si deve rilevare che, sebbene la conservazione dei dati imposta dalla direttiva 2006/24 costituisca un'ingerenza particolarmente grave in tali diritti, essa non è tale da pregiudicare il suddetto contenuto poiché, come deriva dall'articolo 1, paragrafo 2, della stessa direttiva, quest'ultima non permette di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale. Tale conservazione dei dati non è neppure idonea a pregiudicare il contenuto essenziale del diritto fondamentale alla protezione dei dati personali, sancito all'articolo 8 della Carta, considerato che la direttiva 2006/24 prevede, all'articolo 7, una regola relativa alla protezione e alla sicurezza dei dati ai sensi della quale, fatte salve le disposizioni adottate in conformità delle direttive 95/46 e 2002/58, i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione sono tenuti a rispettare taluni principi di protezione e di sicurezza dei dati, principi in base ai quali gli Stati membri assicurano l'adozione di adeguate misure tecniche e organizzative contro la distruzione accidentale o illecita, la perdita o l'alterazione accidentale dei dati».

orientata, alla luce delle disposizioni degli artt. 7 e 8 Carta di Nizza, della direttiva 95/46 (entrata in vigore in momento di transizione dall'analogico al digitale e sicuramente non redatta pensando ad Internet quale ambiente tecnologico privilegiato) trova la sua apoteosi nel percorso argomentativo della pronuncia *Google Spain* oggetto di indagine in questa sede.

Forse è il paragrafo 69 della pronuncia quello che illustra meglio di altri la dichiarazione di intenti dei giudici comunitari in merito alla volontà di leggere le disposizioni rilevanti della direttiva alla luce delle previsioni della Carta a tutela della c.d. *privacy* digitale. I giudici comunitari, in particolare, notano che l'articolo 7 della Carta garantisce il diritto al rispetto della vita privata, mentre l'articolo 8 della Carta proclama espressamente il diritto alla protezione dei dati personali. I paragrafi 2 e 3 di quest'ultimo articolo precisano che «i dati suddetti devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica, e che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente. Tali prescrizioni ricevono attuazione in particolare mediante gli articoli 6, 7, 12, 14 e 28 della direttiva 95/46».

Non si fa fatica a rilevare come la lettura in questione sia talmente orientata da portare ad una sorta di capovolgimento temporale: nel *reasoning* della Corte sono gli artt. 7 e 8, pensati all'inizio di questo millennio, a ricevere attuazione da parte di disposizioni di diritto derivato di cinque anni precedenti.

Partendo da queste premesse, le riflessioni che seguiranno tenteranno di fare emergere le distorsioni, le anomalie o, semplicemente, le rimodulazioni argomentative che sembrano conseguire dalla scelta, da parte dei giudici comunitari, di concentrarsi quasi esclusivamente, nella soluzione del caso, sui parametri forniti dagli artt. 7 e 8 della Carta di Nizza.

La prima anomalia argomentativa è forse la più evidente. A differenza di quanto fatto dall'Avvocato generale, che aveva operato un riferimento numericamente quasi equivalente tra, da una parte, gli articoli appena citati e, dall'altra parte, le disposizioni della Carta rilevanti in tema di libertà di espressione (ed accesso all'informazione) – art. 11 – e di libertà di iniziativa economica – art. 16 –, nell'apparato argomentativo della Corte entrambe le previsioni normative appena richiamate scompaiono.

Nessun riferimento agli artt. 11 e 16 è rinvenibile ed il campo è lasciato interamente libero alle numerosissime citazioni presenti, invece, degli artt. 7 ed 8 della Carta. Non è difficile cogliere un indizio piuttosto

serio di un bilanciamento tra diritti contrastanti che non può non nascere asimmetrico, del tutto sbilanciato, già in partenza, a favore delle ragioni di tutela della *privacy* digitale. Il che, peraltro, è confermato dal passaggio che la Corte ripete più volte¹⁹, in cui, dopo aver ragionevolmente affermato che la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest'ultima occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, «un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta», conclude il ragionamento con una presunzione di prevalenza assai poco comprensibile.

In particolare, rilevando che «se indubbiamente, i diritti della persona interessata tutelati dagli articoli da ultimo citati, prevalgono di norma, anche sull'interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica».

In altre parole, la regola è la soccombenza del diritto (derubricato in mero interesse) all'accesso all'informazione a favore dei diritti che riguardano la protezione della sfera privata e dei dati personali degli utenti, l'eccezione è la possibile prevalenza, in determinati casi ed a certe condizioni, del primo sui secondi.

A ben vedere, però questo rapporto regola/eccezione non solo non figura minimamente nel bilanciamento tra diritti contrastanti proposto dall'Avvocato generale Jääskinen ed era stato già tempo fa esplicitamente escluso dall'Avvocato generale Kokott²⁰ nel caso *Satamedia*²¹, ma è anche agli antipodi rispetto a quanto emerge piuttosto univocamente dalla giurisprudenza rilevante della Corte europea dei diritti dell'uomo. A comincia-

¹⁹ Corte giust., 13 maggio 2014, par. 81 e 97.

²⁰ Conclusioni dell'Avvocato generale Kokott, causa C-73/07, par. 43, in cui si legge che Una rigida applicazione della tutela dei dati potrebbe limitare sensibilmente la libertà di espressione. Così, se i media potessero elaborare e pubblicare informazioni personali solo su consenso o dopo aver avvisato le persone coinvolte, il giornalismo investigativo sarebbe ampiamente escluso. D'altra parte, è evidente che i media possono violare il diritto alla vita privata dei singoli. È pertanto necessario raggiungere un equilibrio ».

²¹ Si v. Corte di giustizia, 16 dicembre 2008, C-73/07, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy*.

re dalla recente decisione *Wgrzynowski e Smolczewski*²² in cui, come è stato sottolineato²³, la Corte di Strasburgo, ribadendo un'impostazione presente fin dalle sue prime grandi decisioni in materia di libertà di espressione, fa chiaramente intendere come la prevalenza di quest'ultima sia la regola e le restrizioni a tale libertà siano eccezioni, che debbono essere interpretate in modo restrittivo.

E ciò anche nel caso in cui il conflitto, come nella fattispecie, sia tra accesso all'informazione sul *web* e interesse del soggetto ricorrente a fare in modo che informazioni pregiudizievoli per la sua reputazione non siano rintracciabili sul *web*²⁴.

Se l'enfaticizzazione del ruolo giocato degli artt. 7 e 8 della Carta riveste un'importanza cruciale in riferimento al preorientamento assiologico con cui la Corte imposta il bilanciamento tra i diritti in conflitto, importanza non minore è assunta dagli stessi parametri quando la Corte, come si diceva, ha proceduto all'applicazione delle disposizioni rilevanti della direttiva 95/46 al caso di specie. Quattro sembrano, in particolare, gli ambiti applicativi in cui maggiore è stato, per così dire, l'effetto manipolativo derivante dalla interpretazione che i giudici comunitari fanno della direttiva alla luce dei più volte richiamati artt. 7 e 8 della Carta.

In primo luogo, la rilevanza, nel caso di specie, della disciplina europea, in secondo luogo la identificazione del motore di ricerca quale *controller*, titolare del trattamento e dunque responsabile dello stesso, in terzo luogo l'applicazione al caso di specie di quanto previsto, da una parte, dall'art. 12, lett. *b* della direttiva che disciplina modalità e ipotesi, *inter alia*, del diritto di ottenere cancellazione, rettifica e congelamento dei dati e, dall'altra, dall'art. 9 della stessa direttiva in materia di deroghe alla disciplina generale in caso di trattamento di dati relativo all'attività giornalistica. Innanzitutto, con riguardo al primo punto evidenziato, è vero che l'Avvocato generale aveva raggiunto la stessa conclusione dei giudici comunitari in merito alla applicabilità delle disciplina europea ad un motore di ricerca che abbia aperto in uno Stato membro, per la promozione e la vendita di

²² Corte eur. dir. uomo, 16 luglio 2013, *Wgrzynowski e Smolczewski c. Polonia* (ric. n. 33846/07).

²³ Si v. G.E. VIGEVANI, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *Danno e responsabilità*, 2014, 7, 742.

²⁴ Nelle riflessioni conclusive si aggiungerà, però, come un trend giurisprudenziale che sembra recentemente accomunare i percorsi interpretativi delle due Corti europee pare portare, attraverso modalità argomentative differenti, all'analogo risultato consistente in una rimodulazione dell'ambito di protezione riconosciuto alla libertà di espressione quando esercitata sul web, rispetto agli standard di tutela ad essa riconosciuta allorché il suo esercizio si esplica nel mondo degli atomi.

spazi pubblicitari, un ufficio che rivolga la sua attività ai cittadini di tale Stato. I giudici di Lussemburgo danno però una giustificazione ultronea rispetto a quella a fondamento del *reasoning* dell'Avvocato generale, argomentando come una interpretazione estensiva della locuzione, prevista dall'art. 4 lett. a), «nel contesto delle attività²⁵ *Google Spain* (che la Corte ammette, non tratta tecnicamente dati)» sarebbe necessaria in quanto «alla luce dell'obiettivo della direttiva 95/46 di garantire una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, con riguardo al trattamento dei dati personali, l'espressione suddetta non può ricevere un'interpretazione restrittiva²⁶». Di nuovo, il diritto alla vita privata diviene prisma esclusivo di modulazione della tutela, senza che si faccia riferimento alla necessaria protezione degli interessi contrastanti. Non solo, ma la Corte, nel tentativo di giustificare tale affermazione, cita, per analogia, nelle sue stesse parole, i punti 62 e 63 della sua precedente pronuncia nel caso *L'Oréal*²⁷. Passaggi che, però, a ben vedere, hanno una limitatissima rilevanza per il caso di specie. Si fa riferimento, infatti, a norme differenti di diritto derivato, in cui è cruciale la protezione, ed i limiti di essa, accordata ai diritti di proprietà industriale e non alla tutela dei dati personali, con un unico riferimento rilevante relativo alla ubicazione extraeuropea dei server²⁸.

In secondo luogo, con riferimento alla identificazione del motore di ricerca quale *controller* del trattamento, in questa sede l'unico aspetto rilevante è quello in cui emerge il peso giocato dal preorientamento assiologico della Corte fondato sull'identificazione degli artt. 7 e 8 quali (quasi) esclusivi parametri di riferimento. E tale peso sembra manifestarsi chiaramente allorché i giudici comunitari, trovandosi ad interpretare l'am-

²⁵ L'articolo 4 della direttiva 95/46, intitolato 'diritto nazionale applicabile', prevede, in particolare, alla lettera a), che ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali effettuato *nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro*.

²⁶ Corte giust., 13 maggio 2014, par. 53.

²⁷ Corte giust., C-324/09, C-324/09, *L'Oréal* e a., citato al par. 53 della sentenza *Google Spain*.

²⁸ *Ibid.*, par. 53 in cui si legge che «come hanno osservato l'avvocato generale al paragrafo 127 delle sue conclusioni e la Commissione nelle sue osservazioni scritte, sarebbe pregiudicata l'efficacia di tali norme qualora l'uso, in un'offerta in vendita o in una pubblicità su Internet destinata a consumatori che si trovano nell'Unione, di un segno identico o simile a un marchio registrato nell'Unione fosse sottratto all'applicazione di tali norme per il solo fatto che il terzo all'origine di detta offerta o pubblicità sia stabilito in uno Stato terzo, che il server del sito Internet da lui utilizzato si trovi in tale Stato o ancora che il prodotto oggetto di detta offerta o pubblicità si trovi in uno Stato terzo».

bito di applicazione dell'art. 2 lett. d) della direttiva che definisce la figura del *controller*, aggiungono che «inoltre, occorre constatare che sarebbe contrario non soltanto al chiaro tenore letterale di tale disposizione, ma anche alla sua finalità — consistente nel garantire, mediante un'ampia definizione della nozione di 'responsabile', una tutela efficace e completa delle persone interessate il fatto di escludere dalla nozione di cui sopra il gestore di un motore di ricerca per il motivo che egli non esercita alcun controllo sui dati personali pubblicati sulle pagine web di terzi (par. 34)».

Qui, l'interpretazione della disciplina rilevante alla luce delle previsioni contenute negli artt. 7 e 8 della Carta ha l'effetto, lungi dall'illuminare il ragionamento della Corte di giustizia, di renderlo più oscuro e debole. Si tratta infatti, come si è avuto modo di evidenziare altrove²⁹, di un'evidente *excusatio non petita*. La Corte cerca di recuperare un'ampia definizione di 'responsabile' dietro una giustificazione, quella di assicurare ampia tutela degli interessati, inconferente. Questo inquadramento trascura che alla posizione di 'responsabile del trattamento', infatti, si collegano gli obblighi che a detta figura fanno capo in base alla direttiva, e che rischiano, se applicati al gestore di un motore di ricerca, di snaturare profondamente il modello di business di questi operatori.

Oltretutto la Corte non chiarisce un aspetto dirimente: per quale fine il responsabile del trattamento stabilisce finalità e strumenti? Se, come i giudici comunitari sostengono, tanto è trattamento quello di chi pubblica dati sulle proprie pagine web quanto lo è quello di chi le indicizza e le riformula in risultati di ricerca, verrebbe da chiedersi allora se anche il gestore del motore di ricerca, estremizzando (ma non troppo) il ragionamento, non debba ottenere il consenso degli interessati.

Se vi fossero ancora dei dubbi sul ruolo giocato dagli artt. 7 e 8 della Carta nella estensione (*melius*: manipolazione) delle maglie normative della disciplina rilevante, fino ad includere nella nozione di responsabile del trattamento anche i motori di ricerca, qualche paragrafo più avanti la Corte ribadisce il concetto argomentando che «nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni

²⁹ M. BASSINI, O. POLLICINO, *Bowling for Columbine. La Corte di giustizia sul caso Google Spain: l'oblio (quasi) prima di tutto?*, in www.diritto24.ilsole24ore.com, 13/05/2014 [consultato 30/09/2014].

della direttiva 95/46, affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata ³⁰lett. b)³¹ e 14, c. 1, lett. b), conferiscano a questi ultimi la possibilità di ottenere dal motore di ricerca la rimozione dai risultati dei collegamenti a pagine web ove siano presenti dati personali, ancorché senza alcuna modifica del sito Internet interessato e senza che la pubblicazione abbia di per sé carattere illecito. Qui viene in gioco in modo diretto l'equilibrio tra, da un lato, la libertà di espressione dei gestori di siti Internet, e, dall'altro, il diritto degli interessati alla tutela dei propri dati personali, ed ai nostri fini è rilevante, in particolare, la forzatura della disciplina prevista dall'art. 12, lett. b), funzionale a piegarla alle esigenze di massima protezione della *privacy* digitale degli interessati. Ai sensi dell'art. 12, lett. b), l'interessato ha diritto di ottenere la cancellazione, la rettifica o il congelamento dei dati, ove il loro trattamento non sia conforme ai principi della direttiva, in particolare a causa del carattere inesatto e incompleto dei dati». La Corte interpreta quest'ultimo inciso a titolo esemplificativo e non esclusivo (come invece sembra emergere da un'interpretazione letterale della disposizione), così ponendo le basi perché qualsiasi difformità nel trattamento in contrasto con la direttiva sia in grado di attribuire all'interessato il diritto di attivarsi come previsto dalla disposizione. Così operando, la sentenza finisce per allargare le maglie della previsione, snaturando il senso del diritto di ottenere la rettifica o la cancellazione dei dati personali, attraverso un richiamo generale alle ipotesi di cui agli artt. 6 e 7 della direttiva.

Al riguardo, tra l'altro, si impone di ricordare che una cosa è un trattamento illecito di dati personali, rispetto al quale i rimedi sono contemplati dalla direttiva, altra è il trattamento senz'altro lecito di dati che l'interessato manifesti l'interesse a non vedere più diffusi in modo incondizionato, che corrisponde specificamente al diritto all'oblio. I due piani paiono confondersi nell'esame della Corte³².

³⁰ Corte giust., 13 maggio 2014, par. 38.

³¹ Come si è avuto modo di rilevare altrove, è altresì forzata la lettura che la Corte di giustizia propone del diritto di opposizione *ex* art. 14, c. 1, lett. b) della direttiva: l'interessato può opporsi in qualsiasi momento al trattamento, per motivi preminenti e legittimi derivanti dalla sua situazione particolare. Anche qui la Corte impropriamente allarga il campo dell'eccezione a detrimento del significato genuino della disposizione: secondo i giudici di Lussemburgo, questa previsione consente agli interessati di far valere tutte le «circostanze caratterizzanti la loro situazione concreta». V. ancora M. BASSINI, O. POLLICINO, *Bowling for Columbine*, cit.

³² Il punto è cruciale importanza. In questo caso la diffusione di una notizia, completa

E la ragione della confusione sembra essere, come più volte evidenziato, la volontà dei giudici comunitari, attraverso una lettura orientata della disciplina rilevante alla luce dell'art. 7 e, specialmente, dell'art. 8 della Carta, di allargare al massimo l'ambito di applicazione della direttiva, fino ad includervi fattispecie abbastanza chiaramente escluse in forza di una interpretazione tanto letterale quanto sistematica della stessa e che possono rientrarvi soltanto grazie ad un'operazione ermeneutica molto simile ad un'attribuzione di un'efficacia diretta ed orizzontale, come si dirà in sede conclusiva, degli articoli della Carta prima citati. Infine, ultimo ambito applicativo della direttiva la cui interpretazione, da parte della Corte, sembra essere stata fortemente influenzata dall'intento di attribuire la massima protezione possibile agli articoli della Carta che compongono lo statuto della *privacy* digitale, è quello relativo all'ipotesi, prevista dall'art. 9 della direttiva, di possibile deroga ai principi generali in essa fissati nell'ipotesi in cui il trattamento dei dati sia finalizzato a scopi giornalistici o di espressione artistica o letteraria. In particolare, la Corte ricorda che, ai sensi del trentasettesimo considerando della direttiva, l'art. 9 della stessa persegue la finalità di conciliare due diritti fondamentali, vale a dire, da un lato, la tutela della vita privata e, dall'altro, la libertà di espressione, quanto che, ai sensi dello stesso art. 9, le deroghe ammesse sono esclusivamente quelle risultino necessarie per conciliare il diritto alla vita privata con le norme

e vera, nel momento della sua pubblicazione, può costituire un trattamento di dati personali in contrasto con la direttiva in quanto, dopo un certo periodo di tempo, tale diffusione non sarebbe più necessaria, vista la sua assenza acquisita di rilevanza sociale. Ci sono almeno due riflessioni da fare al riguardo. La prima; si tratta di un caso diverso rispetto a quello che ha dato luogo alla decisione della Corte di Cassazione, n. 5525 del 2012 che occupa un ruolo fondamentale all'interno del dibattito italiano su protezione e limiti del diritto di oblio. In quel caso, infatti, come ha esattamente ricordato anche recentemente T.E. FROSINI, *Diritto all'oblio e Internet*, in www.federalismi.it, Focus TMT, 6/07/2013 [consultato 30/09/2014], la Cassazione rileva come la notizia in questione «originariamente *completa e vera* diviene non aggiornata, risultando quindi parziale e non esatta, e pertanto non vera». Nel caso *Google Spain*, invece, la notizia non richiedeva un aggiornamento ed unica ragione della sua illegittimità sarebbe quella di essere presente in rete «troppo» a lungo rispetto a quanto sarebbe ragionevole che fosse, tenendo conto del diritto del soggetto coinvolto a non essere ricordato per qualcosa che non sarebbe più di nessuna rilevanza sociale. Mentre nel caso deciso dalla Cassazione il diritto in questione sembra quello di essere ricordati per quello che è effettivamente successo e non soltanto per un segmento di una vicenda (processuale) non aggiornato con il riferimento all'esito definitivo di tale vicenda, nel caso oggetto di indagine in questo contributo il diritto che si fa valere è quello che una notizia vera, completa ed aggiornata sia rimossa dal web, o *melius*, non amplificata in rete attraverso il meccanismo caratterizzante il funzionamento dei motori di ricerca, perché tale amplificazione è in grado di incidere negativamente sulla reputazione del soggetto interessato.

che disciplinano la libertà d'espressione. Ciò nonostante, i giudici comunitari arrivano alla conclusione, non del tutto convincente, ai sensi della quale il trattamento da parte dell'editore di una pagina web, consistente nella pubblicazione di informazioni relative a una persona fisica, può, eventualmente, essere effettuato «esclusivamente a scopi giornalistici» e beneficiare così, a norma dell'articolo 9 della direttiva 95/46, di deroghe alle prescrizioni dettate da quest'ultima, mentre non sembra integrare tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca³³.

La Corte, in altre parole, esclude che il motore di ricerca possa in qualche modo avvalersi della deroga prevista dall'art. 9 della direttiva e, citando la decisione *Satamedia*³⁴ in cui tale deroga è stata oggetto di specifica interpretazione da parte degli stessi giudici comunitari, dimentica però di menzionare quel passaggio in cui quest'ultimi avevano chiarito come il riferimento a trattamenti per scopi giornalistici dovesse essere inteso nel modo più ampio possibile, includendovi qualsiasi «attività diretta a divulgare al pubblico informazioni, opinioni o idee, indipendentemente dal mezzo di trasmissione³⁵».

Ai sensi di tale definizione, è davvero ragionevole la differenziazione, relativa all'applicazione dell'art. 9 della direttiva, che la Corte fa tra editore della pagina *web* e motore di ricerca? Se queste sono state le manipolazioni più evidenti cui sembra aver condotto la lettura costituzionalmente ed 'unidirezionalmente' orientata della Corte, alla luce degli artt. 7 e 8 della Carta, c'è, a ben guardare, anche un che di paradossale in riferimento all'esito cui pervengono i giudici al termine di un *reasoning*, come quello che si è commentato, più che mai *fundamental rights based*.

Attribuire, infatti, un obbligo di rimozione dei link a carico esclusivamente del motore di ricerca, indipendentemente da quello che fa o non fa l'editore del sito web il cui link è indicizzato dal motore stesso, rischia non solo di portare ad una deresponsabilizzazione del primo e ad una responsabilizzazione forse eccessiva del secondo, ma ha come primo effetto quello di fare emergere un contrasto lampante, e paradossale in un apparato argomentativo che fa della tutela di (alcuni) diritti protetti dal *bill of rights* europeo la propria stella cometa, con un principio costituzionale fondamentale che caratterizza il nucleo duro di qualsiasi ordinamento che si fondi sulla *rule of law*. Il riferimento è evidentemente alla necessità di prevedere una riserva di giurisdizione nei casi di una possibile restrizione (in questo caso a seguito di bilanciamento) dei diritti fondamentali in

³³ Corte giust., 13 maggio 2014, par. 85.

³⁴ Corte giust., 16 dicembre 2008.

³⁵ *Ibidem*.

gioco.

Necessità che non sembra essere stata presa in considerazione dalla Corte di giustizia che, in sostanza, delega ad un operatore privato, che però svolge, di fatto, sul web, una funzione pubblica di natura para-costituzionale, di operare quel bilanciamento di interessi che viene teorizzato dalla stessa Corte tra diritto alla *privacy* e diritto ad essere informati. Non possono non tornare alla mente le parole, ricordate ultimamente da Giulio Enea Vigevani³⁶, della Corte europea di diritti nell'uomo nel caso *Wgrzynowski*, prima menzionato, in cui i giudici di Strasburgo hanno occasione di affermare che «non è compito dell'autorità giudiziaria riscrivere la storia, ordinando di far scomparire dal pubblico dominio tutte le tracce di una pubblicazione che pure è stata ritenuta, da sentenze definitive, costituire una ingiustificata violazione della reputazione di un individuo» (par. 65). E non può non riflettersi, conclusivamente a questo riguardo, sul fatto che, a maggior ragione, tale compito non sembra poter essere delegato ad un operatore privato, senza un previo intervento di giudice, e per di più in riferimento ad una notizia vera in cui non vi è mai stato un accertamento giudiziale di suo eventuale carattere diffamatorio.

4. Considerazioni finali

Alla luce dell'analisi fin qui compiuta, non sembrano poterci essere dubbi sul fatto che la Corte di giustizia abbia preso davvero 'sul serio' l'esigenza di tutelare un nuovo *digital right to privacy*, sforzandosi di adeguare alle caratteristiche tecniche del 'mondo dei bit' quel *right to privacy* che Warren and Brandeis, per primi, nel 1890, avevano teorizzato sulla *Harvard Law Review*, pensando, ovviamente, ad un 'mondo di atomi'. Di più: si potrebbe forse aggiungere che nella decisione *Google Spain*, e in quella di poco precedente in materia di *data retention*, più volte richiamata, la questione relativa alla identificazione prima, a dettato normativo invariato, e la protezione poi di tale nuovo diritto (o meglio della nuova collocazione 'digitale' di una pretesa giuridica ben nota) sia stata presa 'eccessivamente' sul serio dai giudici di Lussemburgo. Così sul serio da trascurare le conseguenze negative che un approccio talmente 'dato-centrico', seppure comprensibilmente dettato dallo scandalo mondiale che ha condotto alla rivelazioni sulle intercettazioni da parte della National

³⁶ G.E. VIGEVANI, *Identità, oblio ecc. op. cit.*

Security Agency, rischia, a ben vedere, di avere sul delicato equilibrio alla base dell'ecosistema del web. Due sopra tutte. In primo luogo, la sottovalutazione delle possibili ripercussioni che una radicalizzazione delle (legittime) istanze di tutela del diritto alla protezione dei propri dati personali su Internet, e delle connesse aspettative che tali dati possano, a determinate condizioni, essere rimossi dalla rete, sono in grado di avere sulle altrettanto legittime, e costituzionalmente tutelate, esigenze di tutela di altri diritti fondamentali potenzialmente confliggenti, ad iniziare dalla libertà di espressione.

In secondo luogo, il rischio che tale radicalizzazione abbia l'effetto di attivare prima e consolidare un processo di ipereuropeizzazione, con annesso effetto di balcanizzazione, della regolazione del web. Con riguardo al primo profilo richiamato, se ne è fatto ampio riferimento nell'analisi che precede. La circostanza della totale assenza di citazioni espresse, nel *reasoning* della Corte, dell'art. 11 della Carta è soltanto uno dei tanti indizi che sono stati identificati a conferma del bilanciamento asimmetrico condotto dai giudici di Lussemburgo. Asimmetria, tra l'altro, che ha, come ulteriore conseguenza, quella di condurre ad un minore livello di protezione della libertà di espressione in rete rispetto agli standard di tutela che sono soliti caratterizzare, nella giurisprudenza della Corte, l'esercizio di tale libertà quando il campo di gioco è quello degli atomi e non quello dei bit. Il che, a ben vedere, è una caratteristica che, come si è cercato di dimostrare altrove³⁷, sembra accomunare la giurisprudenza di entrambe le Corti europee. Anche la Corte di Strasburgo, infatti, attraverso differenti tecniche argomentative rispetto a quelle che caratterizzano la giurisprudenza di Lussemburgo, sembra pervenire, nelle sue ultime decisioni, allo stesso risultato: un *downgrading* del livello di protezione della libertà di espressione quando questa è esercitata su Internet³⁸.

Ritornando, invece, alle tecniche argomentative rilevanti nella decisione che si è commentata, è emerso come i giudici comunitari siano pervenuti a tale esito attraverso una lettura manipolativa della disciplina di diritto derivato alla luce dei parametri costituzionali che, agli artt. 7 e 8 della Carta, configurano lo statuto a tutela della c.d. *privacy* digitale.

Di più, pare potersi affermare come il ruolo giocato da tali previsioni nella decisione in commento non sia stato esclusivamente quello di parametro interpretativo della disciplina rilevante. La Corte, nel caso di specie,

³⁷ Sia consentito rinviare a O. POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in www.forumcostituzionale.it, 31/12/2013 [consultato 30/09/2014].

³⁸ Corte eur. dir. uomo, 10 ottobre 2013, *Delfi c. Estonia*, (ric. n. 64569/09) in *Dir. Inf.* 2014, 43 e 242 con note di F. VECCHIO e di R. ALMA.

sembra infatti averne presupposto, non si sa quanto consapevolmente, un'efficacia diretta orizzontale. In particolare, il passaggio rilevante a questo proposito è quello previsto, *inter alia*, dal paragrafo 96 della decisione, laddove la Corte si chiede se l'interessato abbia diritto a che l'informazione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati generato da un motore di ricerca. L'unico modo per rispondere positivamente, come fa la Corte, a tale quesito, essendo l'informazione rilevante in questo caso vera e non parziale, ed essendo il diritto in questione, come l'Avvocato generale ha spiegato in dettaglio nelle sue conclusioni, non enucleabile, *de iure condito*, dalla direttiva 95/46, è quello di attribuire un'efficacia diretta orizzontale all'art. 8 della Carta.

Il punto sembra di cruciale rilievo. Da una parte, infatti, uno sdoganamento della possibilità di attribuire efficacia diretta ed orizzontale ai diritti fondamentali previsti dalla Carta e rilevanti nell'ecosistema digitale sembra in grado di superare quegli ostacoli che fino ad ora hanno impedito di coinvolgere a pieno titolo gli operatori privati nel processo di promozione e tutela degli stessi diritti in Internet; dall'altra, l'importanza di tale applicazione, spesso non tenuta nella dovuta considerazione nel dibattito scientifico, è stata recentemente sottolineata nella relazione annuale per il 2013 della Corte di giustizia³⁹. Il passaggio cruciale, in particolare, sembra quello in cui, nella richiamata relazione, i giudici comunitari sottolineano che «il diritto dell'Unione osta a una prassi giudiziaria che subordina l'obbligo, per il giudice nazionale, di disapplicare ogni disposizione che sia in contrasto con un diritto fondamentale garantito dalla Carta dei diritti fondamentali alla condizione che tale contrasto risulti chiaramente dal tenore della medesima o dalla relativa giurisprudenza, dal momento che tale prassi priva il giudice nazionale del potere di valutare pienamente, se del caso con la collaborazione della Corte di giustizia, la compatibilità di tale disposizione con la Carta medesima».

Con riferimento al secondo profilo di rischio, prima menzionato, connesso alla radicalizzazione di un approccio 'dato-centrico' da parte della Corte di giustizia, ed in particolare ai rischi discendenti da quella che si è definita tendenza ad un'ipereuropeizzazione e frammentazione del diritto di Internet, sono almeno tre le manifestazioni di tale tendenza.

In primo luogo, la sempre più consolidata attitudine ad applicare la disciplina europea in tema di protezione dei dati personali tutte le volte in

³⁹ Disponibile al link http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-03/it_version_provisoire_web.pdf [consultato 30/09/2014].

cui il soggetto interessato sia un cittadino europeo, *melius*, un residente nel territorio dell'Unione, indipendentemente –il che non sarebbe ovviamente una novità, non solo dal luogo in cui si trovano i server da cui ha origine l'attività di trattamento dati, ma anche dalla circostanza, molto meno ovvia, che, tanto sotto il profilo oggettivo dello strumentario rilevante, quanto sotto quello soggettivo dello stabilimento del responsabile del trattamento, il trattamento non sia avvenuto in Europa. A bene vedere, infatti, l'interpretazione estensiva (*melius*: manipolativa) che la Corte, come si è detto in precedenza, ha dato della locuzione nel 'contesto dell'attività' di stabilimento, in forza della quale, di fatto, si considera responsabile del trattamento chi, per la stessa ammissione della Corte, non effettua un trattamento in senso stretto, perviene, in sostanza, a bene vedere, con altro mezzo, allo stesso risultato cui avrebbe portato l'applicazione del nuovo criterio previsto dall'art. 3, c. 2 del Regolamento sulla protezione dei dati personali non ancora approvato⁴⁰. A norma di tale disposizione, infatti, anche se il responsabile del trattamento è stabilito al di fuori dell'Unione, la disciplina europea è comunque applicabile quando le attività del trattamento riguardano l'offerta di beni o la prestazione di servizi ai residenti nell'Unione o il controllo del loro comportamento.

A dettato normativo invariato, e nell'inerzia degli stati membri, l'accelerazione giurisprudenziale di Lussemburgo porta alla confezione di una 'nuova' regola applicabile da subito che anticipa, rendendola di fatto non più necessaria, la futura e più volte posticipata regolamentazione.

Una storia ben nota a chi conosce le dinamiche a trazione giurisprudenziale proprie del processo di integrazione europea. La seconda espressione della tendenza prima identificata ha invece a che fare non con la questione giuridica della legge applicabile, ma con quella per così dire 'fisica' ed 'infrastrutturale' del luogo di conservazione dei dati personali. Si tratta di un tassello ulteriore, abbastanza preoccupante, dell'attitudine, prima menzionata, ad una eccessiva europeizzazione di Internet da parte dei giudici comunitari. Il passaggio rilevante in cui sembra chiaramente manifestarsi lo spostamento dell'attenzione della Corte di giustizia dalla questione relativa alla legge applicabile a quella connessa, invece, alla infrastruttura geografica rilevante, è quello in cui, nella pronuncia, più volte richiamata, che annulla la direttiva in tema di *data retention*, i giudici comunitari hanno modo di affermare che, visto che detta direttiva «non

⁴⁰ Commissione europea, Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), 25 gennaio 2012.

impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta, del rispetto dei requisiti di protezione e di sicurezza, quali richiamati ai due punti precedenti» (par. 68).

In questo caso, il portato normativo del paragrafo 3 dell'art. 8 della Carta è utilizzato dalla Corte per giustificare l'esigenza, non si capisce bene come attuabile in concreto, che i dati personali dei residenti in Europa, trattati al fine di prevenire attentati alla sicurezza nazionale, siano conservati all'interno del territorio degli Stati membri dell'Unione europea. È evidente come la dimensione giuridica della identificazione della legge applicabile e quella geografica del luogo di conservazione dei dati costituiscano due tasselli dello stesso mosaico giurisprudenziale volto a fare della 'legge' e del 'suolo' europei le due colonne portanti per la costruzione di una fortezza continentale a presidio dei dati personali dei residenti in Europa. Fortezza sicuramente inespugnabile all'interno, ma che rischia di non avere quei ponti levatoi che consentano un'effettività extraterritoriale della disciplina europea preposta alla tutela della *privacy* digitale. Sembra proprio questo il limite più evidente del processo in corso ad opera di giudici di Lussemburgo di europeizzazione di Internet, la cui natura transnazionale di portata globale non sembra supportare il successo, con riferimento, appunto, alla effettività della tutela apprestata, di tentativi, seppure comprensibili e financo lodevoli negli intenti, di radicale regionalizzazione della protezione.

Regionalizzazione, quest'ultima, che rischia di trasformarsi, peraltro, e questa è la terza espressione della attitudine prima identificata della Corte di giustizia, in una segmentazione e perfino balcanizzazione dei meccanismi di protezione. Si faccia il caso dell'*enforcement* del c.d. diritto all'oblio. Come *notice and take down*, su scala europea, ma in realtà, in punto di diritto, era esclusivamente *Google Spain* a essere obbligata a prevedere un meccanismo di tutela. Tanto è vero che se la notizia relativa al ricorrente, scintilla da cui è partita la controversia, è ovviamente sparita dalla versione spagnola del motore di ricerca, ma altrettanto non è capitato in tutte le altre declinazioni europee di Google né, tantomeno, in quelle extraeuropee del motore di ricerca.

E' evidente che lo iato tra la natura per forza di cosa territorialmente limitata dell'*enforcement* giurisdizionale e la portata globale del servizio destinatario di tale *enforcement* fa emergere i rischi di un meccanismo di tutela a geometria variabile, con ovvie implicazioni relative, da una parte,

al ribasso del livello di protezione dei diritti in gioco, e, dall'altra, ad una mancata effettività dello stesso meccanismo di tutela.

A guardar bene, non si tratta altro che di un'altra espressione di quella dicotomia *local law* versus *global law* in tema di (*judicial*) *globalitazion*, di cui il diritto di Internet costituisce un campo privilegiato di emersione (e quindi di indagine).

E' stata, ancor più recentemente rispetto alla decisione della corte in *Google Spain*, una pronuncia della Corte suprema dello stato canadese di British Columbia⁴¹ a provare a reagire alle conseguenze, in termini di mancata effettività della tutela, che lo iato e la dicotomia appena identificati portano con sé. E i giudici canadesi lo hanno fatto citando espressamente, tra le altre, anche la decisione della Corte di giustizia oggetto di indagine in queste pagine, a riprova di come il diritto di Internet costituisca, come si è provato ad argomentare altrove⁴², un terreno privilegiato per studiare le dinamiche proprie del c.d. *judicial dialogue*. In particolare la Corte canadese, che aveva a che fare con un caso di concorrenza sleale nel campo della produzione di prodotti *high tech*, ha testualmente concluso che «*an interim injunction should be granted compelling Google to block the defendants' websites from Google's search results worldwide*».

Un ordine di rimozione di portata globale quale reazione all'effetto di segmentazione e frammentazione della tutela connaturato alla, per definizione limitata, dimensione territoriale della *enforcement jurisdiction*⁴³?

Vedremo cosa deciderà la Court of Appeal di British Columbia cui Google ha proposto ovviamente appello nei confronti della decisione appena richiamata. Per una volta, almeno in questo caso, conviene, con attitudine meno eurocentrica rispetto a quello che sembra caratterizzare la prospettiva della Corte di giustizia sul tema, guardare (anche) oltre i confini dell'Unione europea e seguire i futuri sviluppi.

⁴¹ Supreme Court of British Columbia, 13 giugno 2014, *Equustek Solutions Inc. v. Jack*, 2014 BCSC 1063.

⁴² Si v. ancora O. POLLICINO, *Internet nella giurisprudenza*, cit.

⁴³ Si v. U. KOHL, *Jurisdiction and the Internet*, Cambridge, Cambridge University Press, 2007.

Abstract

The article investigates the role played by the relevant provisions of the Charter of Fundamental Rights of the European Union in the reasoning of the «Google Spain» decision of the Luxembourg Court. In particular the paper argues as the asymmetric balance carried out by the said Court finds its genesis in the excessive amplification, in the reasoning of the commented decision, of the scope of application of Articles 7 and 8 of the Charter. An amplification, the above mentioned one, which allows the Court to manipulate the meaning of the directive 95/46 in order to expand its scope of application even to situations which were supposed not to be covered by the said directive according to the intentions of the drafters of the same directive.

Giusella Finocchiaro

Il diritto all'oblio nel quadro dei diritti della personalità

SOMMARIO: 1. Introduzione - 2. Le diverse accezioni del 'diritto all'oblio' - 2.1. Definizione tradizionale - 2.2. Il diritto all'oblio su Internet - 2.3. Il diritto all'oblio nella direttiva europea 96/46 sulla protezione dei dati personali e nella proposta di regolamento europeo generale sulla protezione dei dati del 25 gennaio 2012 - 3. Il diritto all'oblio nella sentenza della Corte di Giustizia - 4. Il diritto all'oblio costituisce un nuovo diritto della personalità?

In questo lavoro si svolgeranno alcune riflessioni sulla nota sentenza della Corte di giustizia del 13 maggio 2014. Per ragioni di sintesi, si assumono i fatti per noti. Quanto ai principi di diritto affermati nella decisione, essi, come ormai si sa, sono tre. In primo luogo, la sentenza afferma che si applica la legge nazionale del Paese nel quale il motore di ricerca opera, esercitando anche altre attività, quali la promozione e la vendita degli spazi pubblicitari. In secondo luogo, che Google, e in generale i motori di ricerca, sono «titolari del trattamento»¹ e pertanto che l'interessato ha il diritto di richiedere che sia rimossa l'indicizzazione direttamente al motore di ricerca, a prescindere da ogni richiesta al gestore del sito *web* che ha pubblicato l'informazione, anche nel caso in cui l'informazione sia stata e sia legittimamente pubblicata sul sito *web*. In terzo luogo, che l'interessato «ha diritto a che l'informazione riguardante la sua persona non venga più collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome» e che «nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato». In questo commento ci si soffermerà, per ragioni connesse all'estensione del presente

¹ Nella traduzione italiana della direttiva è utilizzato il termine 'responsabile' ma, com'è noto, esso equivale al 'titolare', secondo la legge italiana.

lavoro, solo sul terzo punto, che è stato problematicamente qualificato come 'diritto all'oblio' e alla collocazione di questo diritto nell'ambito dei diritti della personalità, nel quadro dell'ordinamento giuridico italiano. Le altre questioni sono oggetto di specifici contributi pubblicati *infra*.

2. Le diverse accezioni del 'diritto all'oblio'

L'espressione 'diritto all'oblio' viene utilizzata in almeno tre differenti accezioni.

2.1. Definizione tradizionale

Una prima accezione è quella più risalente nel tempo, elaborata dalla dottrina civilistica e dalla giurisprudenza, in epoca antecedente all'avvento della Rete.

Con il diritto all'oblio² si è fatto tradizionalmente riferimento al diritto di un soggetto a non vedere pubblicate alcune notizie relative a vicende, già legittimamente pubblicate, rispetto all'accadimento delle quali è trascorso un notevole lasso di tempo. Il diritto all'oblio, in questa accezione, è relativo a vicende che hanno costituito fatti di cronaca o comunque in relazione alle quali la pubblicizzazione, cioè la fuoruscita dalla sfera della riservatezza degli interessati, era da considerarsi lecita. Il problema è «se la persona o le vicende legittimamente pubblicizzate possano sempre costituire oggetto di nuova pubblicizzazione o se, invece, il trascorrere del tempo e il mutamento delle situazioni non la rendano illecita»³. Il diritto

² In dottrina, sul diritto all'oblio si vedano: AA.VV., *Il diritto all'oblio. Atti del Convegno di Studi del 17 maggio 1997*, E. GABRIELLI (a cura di), Napoli, 1999; T. AULETTA, *Diritto alla riservatezza e «droit à l'oubli»*, in ALPA-BESSONE-BONESCHI-CAIAZZA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, pp. 127 e ss.; G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, pp. 801 e ss.; M.R. MORELLI, voce *Oblio (diritto all')*, in *Enc. dir., Agg.*, VI, Milano, 2002; da ultimo, M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009; in giurisprudenza fra le pronunce che si sono occupate più specificamente del diritto all'oblio si segnalano: Cass. civ., 18 ottobre 1984, n. 5259, in *Giur. it.*, 1985, coll. 762; Cass. civ., 9 aprile 1998, n. 3679, in *Foro it.*, 1998, coll. 123 e nel merito Trib. Roma, 15 maggio 1995, in *Dir. Inf.*, 1996, p. 427; Trib. Roma 27 novembre 1996, in *Giust. civ.*, 1997, pp. 1979 e ss. e Trib. Roma, ord. 20.21.27 novembre 1996, in *Dir. aut.*, 1997, pp. 372 e ss.

³ T. AULETTA, *Diritto alla riservatezza ecc. op. cit.*, p. 129.

all'oblio, come magistralmente è stato scritto, appartiene «alle ragioni e 'alle regioni' del diritto alla riservatezza»⁴.

Il tempo gioca un ruolo importante anche qualora non si tratti di eventi di cronaca, ma di eventi in relazione ai quali un periodo significativo sia ormai trascorso e invece manchino elementi di contestualizzazione nel tempo. In questi casi, la giurisprudenza ha ravvisato la violazione del diritto all'identità personale.

2.2. Il diritto all'oblio su Internet

Il diritto all'oblio è mutato con l'utilizzo di Internet e delle reti telematiche, per le modalità proprie di diffusione dell'informazione. Infatti, in Rete la ripubblicazione non è più necessaria, dal momento che per la stessa organizzazione dell'informazione nella Rete l'informazione non è cancellata, ma permane disponibile o quanto meno astrattamente disponibile. In altri termini, non si tratta solo o necessariamente di una ripubblicazione dell'informazione, ma piuttosto di una permanenza della stessa nella Rete.

Muta dunque il ruolo che gioca il tempo e muta l'esigenza che si vuole soddisfare.

il tempo da considerare non è più quello trascorso tra la pubblicazione dell'informazione e la ripubblicazione, ma quello trascorso dal tempo della pubblicazione che perdura.

Non si può fare riferimento al tempo trascorso fra un evento e l'altro, ma invece al tempo di permanenza dell'informazione. Non si tratta di un evento che si ripropone all'attenzione del pubblico, bensì di un evento che potenzialmente non è mai uscito dall'attenzione del medesimo. Siamo di fronte ad un *continuum* temporale e non più a due eventi puntuali.

Anche l'esigenza che in questo caso il diritto vuole soddisfare è diversa.

L'esigenza non è quella di non ripubblicare, ma quella di collocare la pubblicazione, avvenuta magari legittimamente molti anni addietro, nell'attuale presente.

Il problema è quello di attribuire un peso all'informazione, la quale su Internet appare appiattita, con la finalità di garantire che l'identità di un soggetto non sia travisata sulla Rete⁵. L'obiettivo si può raggiungere

⁴ G.B. FERRI, *Diritto all'informazione ecc. op. cit.*, p. 808.

⁵ Questa è la problematica affrontata da V. MAYER-SCHÖNBERGER, *Delete: the virtue of forgetting in the digital age*, Princeton University Press, 2009. Sul tema si rinvia, inoltre, ai miei articoli apparsi in *Dir.Inf.: Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, 2012, pp. 383 e ss. e *La memoria della rete e il diritto all'oblio*,

contestualizzando l'informazione, come ha affermato la recente decisione della Corte di cassazione 5 aprile 2012, n. 5525⁶. Non si tratta del diritto a dimenticare, ma del diritto a contestualizzare⁷.

L'esigenza non è tanto quella di cancellare, ma piuttosto quella di attribuire un peso all'informazione nell'ambito di uno scenario complessivo che vede l'identità come protagonista. Si parla di 'diritto all'oblio', come Cass. 5525/2012 fa, in senso molto lato.

2.3. Il diritto all'oblio nella Direttiva europea 96/46 sulla protezione dei dati personali e nella proposta di Regolamento europeo generale sulla protezione dei dati del 25 gennaio 2012

Una terza accezione del diritto all'oblio è quella che si riferisce al diritto alla cancellazione, al blocco, al congelamento⁸ dei dati o all'opposizione al trattamento dei dati previsti dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 «relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati».

Ivi si dispone, con riguardo al diritto di accesso ai dati da parte della persona interessata, e in particolare nell'art. 12, dedicato al diritto di accesso, che «gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento:

a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi (...)

b) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati».

L'art. 14 della medesima direttiva disciplina il diritto di opposizione della persona interessata e dispone che «gli Stati membri riconoscono alla persona interessata il diritto: *a)* almeno nei casi di cui all'articolo 7, lettere *e)* e *f)*, di opporsi in qualsiasi momento, per motivi preminenti e legitti-

2010, pp. 391 e ss., che riprendo in questo scritto.

⁶ Cass. civ., 5 aprile 2012, n. 5525, in *Foro it.*, 2013, 1, 1, coll. 305.

⁷ Come ha scritto V. ZENO-ZENCOVICH, *Onore e reputazione nel sistema del diritto civile*, Napoli, 1985, p. 120, la decontestualizzazione consiste nella enucleazione dell'immagine di un individuo dal contesto nel quale essa si trovava originariamente e collocazione in uno stato diverso, con l'effetto di creare un contrasto negativo esteriormente percepibile.

⁸ Il termine 'congelamento' ricorre nella direttiva, ma nella legge italiana si utilizza invece il termine 'blocco'.

mi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. In caso di opposizione giustificata il trattamento effettuato dal responsabile non può più riguardare tali dati»⁹. Dall'esame di queste disposizioni muove la decisione della Corte di Giustizia europea in commento.

Le disposizioni della direttiva europea sopra citate sono state attuate nell'ordinamento giuridico italiano con il Decreto legislativo 30 giugno 2003, n. 196, «Codice in materia di protezione dei dati personali» e in particolare con l'art. 7, comma 3, lett. *b*) il quale dispone che «la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati» e con l'art. 7, comma 4 il quale dispone che: «l'interessato ha diritto di opporsi, in tutto o in parte: *a*) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta».

Dunque i due impianti normativi subordinano il diritto alla cancellazione dei dati e il diritto di opposizione al trattamento al ricorrere di precisi presupposti: che il trattamento sia avvenuto in violazione di legge o che ricorrano motivi legittimi. Il quadro non muta nella proposta di regolamento del Parlamento europeo e del Consiglio «concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)» del 25 gennaio 2012¹⁰ ove all'art. 17 si disciplinano il diritto all'oblio e il diritto alla cancellazione dei dati, benché nei commenti la previsione concernente il diritto all'oblio sia stata molto evidenziata ed enfatizzata. I presupposti per richiedere la cancellazione dei dati, secondo il primo comma dell'art. 17 della proposta di regolamento, sono infatti i seguenti:

«*a*) i dati non sono più necessari rispetto alle finalità per le quali sono

⁹ Così l'art. 7: «Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando: (...)

e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, oppure

f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1».

¹⁰ COM 2011 (12) final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_it.pdf, [visualizzato il 20/07/2014] .

stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si fonda il trattamento, di cui all'articolo 6, paragrafo 1, lettera *a)*, oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattare i dati;

c) l'interessato si oppone al trattamento di dati personali ai sensi dell'articolo 19;

d) il trattamento dei dati non è conforme al presente regolamento per altri motivi».

Dunque nessuna innovazione sostanziale in questo comma, essendo la lettera *a)* riconducibile al noto principio di necessità, la lett. *b)* un'applicazione della revocabilità del consenso, la lettera *c)* una conferma del previgente art. 14 della direttiva, la lettera *d)* un'applicazione dell'art. 12 della direttiva e comunque dei principi generali di cui all'art. 6¹¹.

L'innovazione è, a ben vedere, nel secondo comma dell'art. 17 ove si configura una nuova responsabilità del titolare del trattamento, prevedendo che il titolare del trattamento¹² debba informare i terzi che stanno trattando i dati della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali e che, se il titolare ha autorizzato un terzo a pubblicare dati personali, è ritenuto responsabile di tale pubblicazione.

Tuttavia giova ricordare che un analogo obbligo del titolare di informare i terzi era già presente nella legge italiana. Volendo meglio delineare i confini di termini dal significato limitrofo, quali cancellazione dei dati e oblio¹³, si può definire la cancellazione come un'operazione sui dati che

¹¹ In questo stesso senso ICRI Working Paper Series, *Search engines after Google Spain: internet@liberty or privacy@peril?*, B.VAN ALSENOY – A.KUCZERAWY – J.AUSLOOS (ed.), no. 15, Interdisciplinary Center for Law and ICT, K.U. Leuven, 2013, p. 43. Sulla rubrica dell'articolo, «diritto all'oblio e alla cancellazione», non tanto infelice, ma piuttosto politicamente orientata nel dibattito Europa — Stati Uniti, v. le riflessioni di F.PIZZETTI, *Il prisma del diritto all'oblio*, in AA.VV., *Il caso del diritto all'oblio*, F.PIZZETTI (a cura di), Torino, 2013, pp. 21 e ss. In commento all'art. 17 del regolamento v.M. SIANO, *Il diritto all'oblio in Europa e il recente caso spagnolo*, *ivi*, p. 123. Nello stesso senso, A.MANTELERO, *Il diritto all'oblio dalla carta stampata ad Internet*, *ivi*, p. 166.

¹² Anche in questo caso, nella versione italiana del regolamento è utilizzato il termine 'responsabile' ma, com'è noto, è da intendersi 'titolare'.

¹³ Dalla ricostruzione di G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 310, benché riferita alla l. 31 dicembre 1996, n. 675, sembra intendersi che il diritto all'oblio sia da riferirsi ai dati di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati, mentre l'opposizione al trattamento va riferita al caso in cui il trattamento sia effettuato in modo lecito e l'interessato possa prospettare ragioni particolari meritevoli di protezione (p. 314). La

esclude ogni ulteriore conservazione degli stessi, mentre l'oblio sembra piuttosto essere una finalità, che si può raggiungere con la cancellazione, ma anche con il blocco.

3. Il diritto all'oblio nella sentenza della Corte di Giustizia

La sentenza in commento si esprime, in via pregiudiziale, sull'interpretazione degli artt. 12 e 14 della direttiva 95/46/CE, sopra richiamati, aventi rispettivamente ad oggetto l'accesso ai dati e l'opposizione al trattamento. In particolare, la Corte è chiamata ad esprimersi sull'interpretazione dell'art. 12, lett. *b*) ove si dispone che «gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento: (...) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati» e dell'art. 14, primo comma, lett. *a*) ove si dispone che «gli Stati membri riconoscono alla persona interessata il diritto: (...) almeno nei casi di cui all'articolo 7, lettere *e*) e *f*), di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale».

Dunque il contenuto del diritto all'oblio indagato è quello proprio della terza accezione sopra individuata: il diritto alla cancellazione, al congelamento dei dati e all'opposizione al trattamento.

Questi diritti, com'è noto, secondo la conclusione cui giunge la Corte, possono essere fatti valere anche nei confronti del motore di ricerca, che costituisce un titolare di trattamento.

Il motore di ricerca non potrà evidentemente cancellare i dati personali che si trovano presso il titolare di trattamento che ha pubblicato l'informazione (ad esempio, sul sito dell'editore del giornale, nei molti casi verificatisi) ma soltanto il collegamento a detti dati, i quali ben potranno permanere presso il titolare del trattamento. Si realizzerà così una sorta di

distinzione fra cancellazione e blocco è operata da R. IMPERIALI – R. IMPERIALI, *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Milano, 2004, p. 93, secondo i quali qualora al titolare venga lasciata la scelta di optare fra cancellazione e blocco, questi dovrebbe procedere con la cancellazione, se si tratta di violazione insanabile di legge, per poi procedere alla sospensione, se si tratta di violazione riparabile, in modo da consentire successivamente la ripresa del trattamento.

diritto a non essere trovato *online* piuttosto che un vero e proprio diritto all'oblio¹⁴, inteso quest'ultimo nel senso di diritto alla cancellazione dei dati. Pare a questo punto opportuno ripercorrere, se pur in modo sintetico, il percorso argomentativo della Corte. La domanda del giudice del rinvio era, sul punto, la seguente¹⁵: «Per quanto concerne la portata del diritto di cancellazione e/o opposizione al trattamento di dati in relazione al diritto all'oblio, si chiede: se si debba ritenere che i diritti di cancellazione e congelamento dei dati, disciplinati dall'articolo 12, lettera b), e il diritto di opposizione al loro trattamento, regolato dall'articolo 14, [primo comma,] lettera a), della direttiva [95/46], implicino che l'interessato può rivolgersi ai motori di ricerca per impedire l'indicizzazione delle informazioni riguardanti la sua persona pubblicate su pagine *web* di terzi, facendo valere la propria volontà che tali informazioni non siano conosciute dagli utenti di Internet, ove egli reputi che la loro divulgazione possa arrecargli pregiudizio o desideri che tali informazioni siano dimenticate, anche quando si tratti di informazioni pubblicate da terzi lecitamente». Con questa domanda si pongono in realtà due diversi quesiti: se l'interessato possa rivolgersi direttamente al motore di ricerca invece che al soggetto che ha pubblicato l'informazione *online* e se il presupposto della domanda possa essere costituito dalla considerazione che la divulgazione arrechi pregiudizio o dal desiderio che le informazioni siano dimenticate. Al primo quesito la Corte risponde affermativamente, argomentando, come è noto, che il motore di ricerca è titolare del trattamento dei dati. In relazione al secondo quesito la Corte ritiene che «quanto all'articolo 12, lettera b), della direttiva 95/46, la cui applicazione è subordinata alla condizione che il trattamento di dati personali sia incompatibile con la direttiva stessa, occorre ricordare che, come si è rilevato al punto 72 della presente sentenza, un'incompatibilità siffatta può derivare non soltanto dal fatto che tali dati siano inesatti, ma anche segnatamente dal fatto che essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici»¹⁶. E aggiunge che pertanto «anche un trattamento inizialmente lecito di dati esatti può divenire, con il tempo, incompatibile con la direttiva suddetta qualora

¹⁴ In questo senso molti commenti statunitensi che si riferiscono al «right not to find». Anche SIANO, *Il diritto all'oblio in Europa e il recente caso spagnolo*, cit., p. 132, ritiene che meglio sarebbe stato riferirsi al «right not to be seen».

¹⁵ Punto 20 della sentenza, terza questione pregiudiziale.

¹⁶ Punto 92 della sentenza.

tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura in particolare nel caso in cui i dati risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso»¹⁷. E conclude che «l'inclusione nell'elenco di risultati — che appare a seguito di una ricerca effettuata a partire dal suo nome — dei *link* verso pagine *web*, legittimamente pubblicate da terzi e contenenti informazioni veritiere relative alla sua persona, è, allo stato attuale, incompatibile con il citato articolo 6, paragrafo 1, lettere da *c*) a *e*), a motivo del fatto che tali informazioni appaiono, alla luce dell'insieme delle circostanze caratterizzanti il caso di specie, inadeguate, non pertinenti o non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento in questione realizzato dal gestore del motore di ricerca, le informazioni e i *link* in parola di cui al suddetto elenco di risultati devono essere cancellati»¹⁸.

Dunque la Corte afferma il diritto a cancellare i dati se essi sono inadeguati, non pertinenti o non più pertinenti in rapporto alle finalità del trattamento¹⁹. Non si tratta di un diritto *ad nutum* ma di un diritto a cancellare che va ponderato ed esercitato in ragione delle caratteristiche dei dati costituite dall'adeguatezza, dalla pertinenza o dalla non pertinenza del trattamento rispetto alle finalità. Non viene affermato un generale diritto all'oblio sui dati trattati dai motori di ricerca, ma l'applicabilità anche a questi di quanto disposto nella direttiva²⁰. Non si tratta del diritto a cancellare i dati *tout court*. «Di per sé, una preferenza soggettiva non costituisce un motivo preminente e legittimo ai sensi dell'art. 14, lett. *a*), della direttiva»²¹. Questa affermazione della Corte appare condivisibile e sostanzia una specificazione di quanto disposto nella direttiva. D'altro canto, essa solleva nuovi interrogativi. Se, infatti, l'oggetto della cancellazione è costituito dai *link* pubblicati del motore di ricerca (non dai dati

¹⁷ Punto 93 della sentenza.

¹⁸ Punto 94 della sentenza.

¹⁹ In questo senso G. BUSIA, *Le operazioni dei motori di ricerca su internet vanno ricondotte al concetto di 'trattamento'*, commento a Corte di giustizia dell'Unione europea - Grande Sezione - Sentenza 13 maggio 2014 Causa C-131/12, in *Guida dir.*, 24, 2014, pp. 15 e ss.

²⁰ Così F. PIZZETTI, in *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, <http://www.federalismi.it/AppIOpenFilePDF.cfm?artid=26322&dpath=document&dfile=10062014174108.pdf&content=La+decisione+della+Corte+di+giustizia+sul+caso+Google+Spain:+pi%C3%B9+problemi+che+soluzioni+-+stato+-+dottrina+->, pubblicato il 06/06/2014 [consultato 30/09/2014].

²¹ Così le conclusioni dell'Avvocato generale Niilo Jääskinen, in appendice a questo volume punto 108.

pubblicati dal gestore del sito fonte dell'informazione) e le finalità del trattamento sono quelle del motore di ricerca, occorre interrogarsi sulle conseguenze di questa affermazione²².

È in rapporto alle finalità del motore di ricerca che va effettuata la valutazione sull'adeguatezza, la pertinenza o la non pertinenza dei dati e conseguentemente assunta la decisione di cancellare.

Gli interessi legittimi perseguiti dai motori di ricerca sono quelli di facilitare l'accesso alle informazioni per gli utenti di Internet, migliorare l'efficacia della diffusione delle informazioni su Internet, consentire diversi servizi della società dell'informazione²³. Questi interessi corrispondono a tre diritti fondamentali tutelati dalla Carta dei diritti fondamentali dell'Unione europea: libertà di informazione, libertà di espressione e libertà di impresa²⁴.

Nell'effettuare il trattamento, il motore di ricerca deve rispettare i principi di qualità dei dati dettati dalla direttiva: in particolare «i dati personali debbono essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite, ed aggiornati, vale a dire non obsoleti per i fini per i quali sono stati rilevati»²⁵. Alla luce del principio della qualità dei dati sopra menzionato va interpretata l'affermazione della Corte, invero non particolarmente felice, secondo la quale «la constatazione di un diritto siffatto non presuppone che l'inclusione dell'informazione in questione nell'elenco di risultati arrechi un pregiudizio all'interessato»²⁶. Il *legal reasoning* della Corte è correttamente svolto entro i confini delineati dalla direttiva, ma la prospettiva non può essere limitata all'applicazione della direttiva.

Il bene giuridico che si vuole tutelare è quello dell'identità. Il dato personale è, in ultima analisi, inadeguato o non pertinente rispetto all'identità di un soggetto. Il motore di ricerca è, infatti, idoneo a generare una vera e propria immagine *online*.

²² Appare condivisibile quanto affermato da F. PIZZETTI, in *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, cit., cioè che la qualificazione dei motori di ricerca come titolari di trattamento apra scenari molteplici e particolarmente complessi.

²³ Così le conclusioni dell'Avvocato generale, cit., punto 95. Per un primo commento O. POLLICINO- M. BASSINI, *Il diritto all'oblio a Lussemburgo*, in *Diritto*24, 2014. Ritenendo questi interessi legittimi perseguiti con il trattamento, l'Avvocato generale legittima il trattamento senza consenso dell'interessato.

²⁴ Così ancora le conclusioni dell'Avvocato generale, cit., punto 95.

²⁵ Così ancora le conclusioni dell'Avvocato generale, cit., punto 96.

²⁶ Punto 96 della sentenza.

4. *Il diritto all'oblio costituisce un nuovo diritto della personalità?*

Non pare che il diritto all'oblio costituisca un diritto in sé e che si debba ampliare il catalogo dei diritti della personalità, dal momento che esso appare comunque strumentale, o al diritto all'identità personale o al diritto alla protezione dei dati personali. Da un punto di vista metodologico, non serve in questo caso procedere alla creazione e alla formulazione di un nuovo diritto, dal momento che i diritti già consolidati sono idonei ad accogliere le esigenze nuove²⁷.

Invero, se si considerano le prime due accezioni sopra illustrate del diritto all'oblio, esso appare strumentale al diritto all'identità personale. Infatti, la prima accezione del diritto all'oblio è che esso costituisca un diritto a non vedere ripubblicata l'informazione rispetto alla cui prima pubblicazione è trascorso un rilevante periodo di tempo, qualora la riproposizione della notizia non sia di attuale interesse. La seconda accezione del diritto all'oblio lo riconduce alla contestualizzazione dell'informazione.

Il bene giuridico tutelato è in entrambi i casi quello dell'identità personale. Si tratta del diritto a non vedere travisata la propria immagine sociale. Ed è un fatto, che non abbisogna di dimostrazioni, che il motore di ricerca crei l'immagine *online* di un soggetto, non meno vera solo perché si trova su Internet. Certo non è questa la finalità del trattamento dei dati effettuato dal motore di ricerca, finalità piuttosto costituita dal rendere l'informazione reperibile su Internet. Tuttavia la creazione di un'immagine *online* è certamente un effetto dell'attività svolta dal motore di ricerca. Dunque in questi due casi, il diritto all'oblio è strumentale alla tutela del diritto all'identità personale. Se si considera la terza accezione del diritto all'oblio, cioè il diritto a cancellare i dati, il bene giuridico tutelato è costituito dai dati personali. In questo caso, che è peraltro quello considerato dalla direttiva europea, dalla legge italiana, dalla proposta di regolamento europeo, nonché dalla decisione della Corte di giustizia in commento, il bene giuridico considerato è quello della protezione dei dati personali. In questo caso, il diritto a cancellare è strumentale al diritto alla protezione dei dati personali. Il dato personale può essere cancellato, come afferma la Corte, se non è più adeguato, aggiornato o pertinente.

Vero è che i due diritti in considerazione, il diritto all'identità personale e il diritto alla protezione dei dati personali sono diritti molto vicini e

²⁷ F. PIZZETTI, *Il prisma del diritto all'oblio*, cit., p. 22 con ampia nota, Evidenza che «si tratta di categorie più evocative che descrittive, che spesso trovano nel fascino stesso della loro formulazione una seduzione particolare».

volti a tutelare un unico bene: quello dell'identità della persona. Infatti, lo scenario e la prospettiva non sono quelli del dato personale contenuto nel singolo archivio, bensì quelli della tutela della persona nella rete Internet, che non è un archivio ma un deposito²⁸, la quale crea, attraverso i motori di ricerca l'immagine della persona.

Indipendentemente dalla constatazione che le informazioni sulla persona *online* siano state lecitamente pubblicate, l'immagine complessiva può dare luogo ad un travisamento della sua immagine sociale. Come scrive la Cassazione: «La notizia, originariamente *completa e vera*, diviene *non aggiornata*, risultando quindi *parziale e non esatta*, e pertanto sostanzialmente *non vera*»²⁹. Il diritto alla protezione dei dati personali e i diritti della personalità ad esso limitrofi, quali il diritto all'identità personale, il diritto di rettifica, il diritto alla riservatezza, il diritto alla protezione dei dati personali, il diritto alla reputazione, il diritto all'immagine e il diritto al nome, sono tutti volti a tutelare un unico bene giuridico: l'identità. Identità che viene vista nelle sue molteplici forme ed espressioni: le informazioni concernenti un soggetto, la sua immagine sociale, la sua immagine sulla stampa, la sua immagine fisica, il suo nome.

Così il diritto all'identità personale consiste nel diritto di vietare un travisamento dell'immagine sociale di un soggetto; il diritto di rettifica comporta una forma di controllo sull'immagine sociale di un soggetto e il diritto, per questi, di fare correggere le pubblicazioni lesive o contrarie a verità; il diritto alla riservatezza comporta un controllo del soggetto sulle vicende e sulle informazioni che lo riguardano; il diritto alla reputazione tutela la stima sociale di un soggetto; il diritto al nome va inteso come strumento di identificazione di un soggetto e quindi, per traslato, strumento di tutela dell'identità; il diritto all'immagine può anche essere inteso in senso lato, come tutela dell'immagine sociale, oltre che dell'immagine fisica di un soggetto³⁰.

Il bene giuridico complessivamente tutelato è uno solo, quello dell'identità, declinata nei suoi molteplici aspetti e nelle sue molteplici forme.

²⁸ Si riferisce ad Internet come 'deposito' l'Avvocato generale nelle sue conclusioni, *cit.*, punto 27. V. inoltre il mio *La memoria della rete e il diritto all'oblio*, *cit.*

²⁹ Così Cass. civ., 5 aprile 2012, n. 5525, *cit.*, in corsivo nel testo della sentenza.

³⁰ Così V. ZENO-ZENCOVICH, voce *Identità personale*, in *Dig. it., Sez. Civ.*, IX, Torino, 1995. Si rinvia, inoltre, a G. FINOCCHIARO, voce *Identità personale*, in *Dig. disc. priv.*, Sez. civ., Torino, 2010, pp. 721 e ss. e a G. RESTA, *Identità personale e identità digitale*, in *Dir. Inf.* 2007, pp. 511 e ss. Ritiene che si dissolvano i confini tra le singole situazioni soggettive e si definisca un generale potere di controllo sulla circolazione commerciale dell'identità, G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 166.

E un ulteriore elemento di complessità è oggi aggiunto dalla possibilità di manifestare l'identità anche con mezzi digitali e di assumere, nel mondo virtuale, molteplici identità³¹.

Ma se l'identità è sintesi dei tanti elementi di natura diversa che la compongono, essa non è certo una sintesi statica. Il tempo gioca un ruolo essenziale: la persona è ciò che è in un determinato momento storico e l'identità muta col tempo. Divengono essenziali la contestualizzazione e la storicizzazione. Eventi occorsi in una certa epoca possono non corrispondere più alla personalità di un soggetto in un diverso momento storico. Sul terreno di questo conflitto, fra la verità della storia e l'identità attuale, nasce il diritto all'oblio.

Naturalmente, tale diritto deve essere oggetto di bilanciamento con altri diritti, quali il diritto all'informazione. La Corte di giustizia afferma che in linea generale il diritto alla protezione della vita privata e il diritto alla protezione dei dati personali devono prevalere, salvo che si tratti di soggetti che ricoprono un ruolo pubblico³², ma questa affermazione appare apodittica e destinata a trovare molte correzioni e precisazioni. Come ricordato nelle conclusioni dell'avvocato generale, agli interessi legittimi dei motori di ricerca corrispondono tre diritti fondamentali tutelati dalla Carta dei diritti fondamentali dell'Unione europea: libertà di informazione, libertà di espressione e libertà di impresa³³. «L'accessibilità universale delle informazioni su Internet dipende dai motori di ricerca, dato che trovare informazioni rilevanti senza di essi sarebbe troppo complicato e difficile e produrrebbe risultati limitati»³⁴. Internet è oggi un gigantesco deposito e non un archivio ordinato³⁵.

³¹ Sull'argomento RODOTÀ, *La vita e le regole. Tra diritto e non diritto*, Milano, 2006.

³² Così la decisione: «Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi».

³³ Così le conclusioni dell'Avvocato generale, *cit.*, punto 95.

³⁴ Così le conclusioni dell'Avvocato generale, *cit.*, punto 45.

³⁵ Critici sulla decisione che ritengono sia applicabile ad Internet solo nel medio termine, P. DE HERT e V. PAKONSTANTINO, *How the European Google Decision May Have Nothing To Do With a Right to Be Forgotten*, in <https://www.privacyassociation>.

Ogni soluzione passerà inevitabilmente per un complesso processo di bilanciamento di diritti: quanto meno il diritto di accesso ad Internet, che senza i motori di ricerca è fortemente depotenziato, il diritto alla libertà di espressione, che rende il diritto all'oblio assai arduo da comprendere oltreoceano³⁶, e il diritto alla libertà di impresa e necessariamente si tratterà di una valutazione da effettuarsi caso per caso.

Abstract

This article examines the so called «right to oblivion» as stated by the European Court of Justice. The main question is whether the right to oblivion constitutes a new right under Italian law. In order to answer this question the paper analyzes the possible meanings of the expression «right to oblivion». The conclusion reached is that the right to oblivion is not a new right, but only an instrument to realize other well-known rights such as the right to personal data protection and the right to not have one's own social Image misrepresented. This right needs to be balanced with other fundamental rights.

org/privacy_perspectives/post/how_the_europe_an_google_decision_may_have_nothing_to_do_with_a_right_to_be, pubblicato il 19/06/2014 [consultato 30/09/2014]. Critico altresì C.KUNER, *The Court of Justice of EU's Judgment on the 'Right to be Forgotten': An International Perspective*, in <http://www.ejiltalk.org/the-court-of-justice-of-eus-judgment-on-the-right-to-be-forgotten-an-international-perspective/>, pubblicato il 20/05/2014 [consultato 30/09/2014], il quale ritiene che la decisione possa creare una rete Internet europea, in contrapposizione a quella mondiale.

³⁶ Per una sintesi delle due diverse visioni, europea ed italiana, v. J. ROSEN, *The Right to be Forgotten*, in *Stanford Law Review Online*, 2012, in <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten>, [consultato il 20/07/2014].

Giandonato Caggiano

L'interpretazione del criterio di collegamento del 'contesto delle attività di stabilimento' dei responsabili del trattamento dei dati personali

SOMMARIO : 1. Oggetto del contributo - 2. Elementi essenziali dello stabilimento nel diritto dell'Unione - 3. I pareri del WG 29 sull'attività dei motori di ricerca e sull'applicazione del diritto nazionale - 4. Le richieste del giudice del rinvio e la posizione dell'Avvocato generale - 5. L'interpretazione della Corte di giustizia - 6. La proposta di regolamento della Commissione sulla tutela dei dati personali - 7. Il criterio di collegamento dell'attività diretta nella scelta della legge applicabile al contratto del consumatore e il criterio del «centro di interessi» del consumatore per la determinazione della competenza giurisdizionale - 8. Cenni alla giurisprudenza sulla responsabilità degli ISP 'attivi' e 'passivi'

1. Oggetto del contributo

L'oggetto del presente contributo riguarda il ruolo dello stabilimento di un'impresa responsabile del trattamento di dati personali al fine dell'applicazione territoriale delle norme nazionali di attuazione della direttiva 95/46 sulla tutela dei dati personali¹. La questione è analizzata nella prospettiva della giurisprudenza sulla responsabilità civile degli Internet Service Provider (ISP), la cui attività tende a standardizzarsi in modelli non conosciuti al momento dell'adozione delle direttive 95/46 e 2000/31 sul commercio elettronico². La prima delle questioni, esaminate

¹ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, *GUCE* L 281, 23 novembre 1995, pp. 31 ss. Per la tecnica di armonizzazione minimale adottata, la direttiva 95/46 lascia agli Stati membri un margine di discrezionalità che determina l'esistenza di leggi nazionali di attuazione diversificate fra di loro.

² Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici del commercio elettronico nel mercato interno («direttiva sul commercio elettronico»), *GUCE* L 178, 17.7.2000. Le consultazioni svolte su una possibile revisione di tale direttiva hanno avuto esito negativo, v. Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce (2000/31/EC), 2010 e Summary of the results sul sito

dalla Corte di giustizia nella sentenza *Google Spain*, riguarda l'applicazione delle norme nazionali di attuazione della direttiva 95/46 alle attività di un ISP che opera quale motore di ricerca in una posizione monopolistica a livello dell'Unione in tale mercato di servizi. Com'è noto, le attività del Gruppo Google sono svolte, in parte, dalla società madre stabilita in un Paese terzo (California/Usa) che indicizza e archivia le ricerche sul web; in parte, dagli stabilimenti/filiali in vari Stati membri dell'Unione che offrono l'interfaccia del servizio di ricerca agli utenti di uno Stato membro³ e gestiscono la pubblicità diretta al mercato nazionale tramite una serie di link sponsorizzati dalle imprese (posizionamento *Google's AdWords*). Com'è noto, proprio quest'ultimo meccanismo rende economicamente sostenibile il modello di business di Google e consente di considerare l'attività del motore di ricerca come prestazione di un servizio ai sensi del diritto dell'Unione, anche se la remunerazione non proviene direttamente dall'utente ma dai prestatori della comunicazione pubblicitaria. Dal momento che l'interpretazione della Corte di giustizia tiene conto ampiamente della posizione del WG Art. 29, il cui segretariato è gestito dalla Commissione europea, sembra opportuno partire dalle riflessioni di questo autorevole organo di consulenza che si avvale dell'esperienza e del parere delle Autorità-garanti degli Stati membri. Merita un accenno anche la posizione dell'Avvocato generale, che viene accolta dalla Corte sul punto in esame, diversamente che sulle altre questioni esaminate.

Il presente contributo si interroga anche sulle prospettive di impatto della sentenza *Google Spain* sulla ormai prossima adozione della proposta di regolamento generale sulla protezione dei dati personali che sostituirà la direttiva 95/46⁴. L'interpretazione della Corte non rischia di diventare presto obsoleta dal momento che, allo stato dell'iter di adozione, il Consiglio e Parlamento europeo appaiono intenzionati a riaffermare il criterio delle attività svolte all'interno dello stabilimento del responsabile del trattamen-

della DG Mercato interno e servizi. Sul tema specifico delle procedure di rimozione di contenuti illeciti, v. Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, 2012 (reperibile on line sul medesimo sito).

³ Il servizio Google Search opera a livello mondiale tramite il sito web «www.google.com» ed è gestito da Google Inc., società madre del gruppo con sede sociale negli Stati Uniti. In ciascun paese dove esiste uno stabilimento, il sito di ricerca possiede un dominio diverso. È facile verificare che l'uso delle stesse parole chiave su domini nazionali Google diversi può determinare la visualizzazione di risultati e annunci pubblicitari diversi.

⁴ COM(2012) 11 final, 25.1.2012, Proposta di regolamento del Parlamento europeo e del Consiglio, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati).

to nell’Unione (art. 3, par. 1 della proposta di regolamento). Tuttavia considerato che l’adozione di un regolamento renderà uniforme il diritto degli Stati membri, la questione non si porrà più, come accade attualmente, in relazione l’applicazione della legge nazionale (di attuazione della direttiva) dei singoli Stati membri, ma riguarderà l’applicabilità *tout court* del nuovo regolamento ai responsabili di trattamento-dati non-stabiliti nello Spazio economico europeo (SEE).

2. Elementi essenziali dello stabilimento nel diritto dell’Unione

È importante sottolineare che l’attività del motore di ricerca Google ben potrebbe svolgersi sotto forma di prestazione di servizi senza alcun obbligo di stabilimento. La costituzione di filiali in alcuni Stati membri corrisponde solo ad autonome scelte di politica di sviluppo industriale del Gruppo all’interno dell’Unione, soprattutto in relazione ai rapporti con la raccolta di comunicazione pubblicitaria rivolta al mercato nazionale di riferimento della filiale.

Vale la pena pertanto di ricordare alcune nozioni sul diritto di stabilimento⁵ che, nella dinamica con la libera prestazione dei servizi, garantisce la mobilità delle imprese e dei professionisti nel territorio dell’Unione. Il principio del diritto dell’Unione è quello secondo cui le persone fisiche che esercitano attività autonome e le persone giuridiche che operano legalmente in uno Stato membro possono esercitare un’attività economica in un altro Stato membro, diverso da quello in cui sono stabiliti, su base stabile e continuativa (art. 49 del TFUE) e prestare, così, servizi a livello transfrontaliero pur conservando il loro stabilimento nel loro paese d’origine (art. 56 del TFUE).

Il diritto di un operatore economico stabilito in uno Stato membro di fornire servizi in un altro Stato membro non è condizionato allo svolgimento di servizi identici o simili. L’unica condizione richiesta è il carattere transfrontaliero della prestazione, vale a dire che il prestatore sia stabilito in uno Stato membro diverso da quello del destinatario. Il Trattato non prevede durata, frequenza o tipologia di servizi che determinino un automatico trasferimento dello stabilimento di un’impresa da uno Stato ad un

⁵ Per una prospettiva di diritto comparato, A. GUACCERO, *Libertà di stabilimento e diritto societario degli Stati membri: Europa vs USA*, in *Europa e diritto privato*, 2007, pp. 133 e ss.

altro Stato⁶. L'unico criterio determinante è l'esistenza di un'infrastruttura che consenta di esercitare in maniera stabile e continuativa un'attività professionale e di offrire i servizi anche ai cittadini di un altro Stato membro⁷. Inoltre, la circostanza che un'impresa sia stabilita in uno Stato per avvantaggiarsi di una legislazione nazionale più favorevole non preclude che le relative attività possano essere considerate 'servizi' ai sensi del Trattato, dal momento che l'esercizio di una libertà fondamentale non costituisce in sé un abuso⁸.

L'art. 49 TFUE qualifica il divieto alla restrizione alla libertà di stabilimento come un obbligo di trattamento non discriminatorio rivolto agli Stati membri: sia nei confronti dei cittadini di un altro Stato membro sia per l'apertura di agenzie, succursali o filiali. Le società costituite conformemente alla legislazione di uno Stato membro e aventi la sede sociale, l'amministrazione centrale o il centro di attività principale all'interno dell'Unione, sono equiparate ai fini dell'applicazione delle disposizioni sulla libertà di stabilimento, alle persone fisiche aventi la cittadinanza degli Stati membri. La medesima norma chiarisce che per società si intendono sia quelle di diritto civile e commerciale, ivi comprese le società cooperative, sia le altre persone giuridiche contemplate dal diritto pubblico o privato ad eccezione delle società che non si prefiggono scopi di lucro.

3. I pareri del WG29 sull'attività dei motori di ricerca e sull'applicazione del diritto nazionale

Come abbiamo già detto, un rilevante contributo al consolidamento dell'interpretazione dei criteri di collegamento in materia di trattamento dei dati personali è quello dato in questi ultimi anni dal Gruppo di lavoro

⁶ Sentenze 11 dicembre 2003, *Bruno Schnitzer*, C-215/01, Raccolta, I-14847, punti 30-31, nonché 10 maggio 2012, *Duomo Gpa Srl*, Cause riunite C-357/10 a C-359/10, non ancora pubblicata in Raccolta, punto 32. In dottrina, v. per tutti R. MASTROIANNI, *Libera circolazione dei servizi*, in G. STROZZI (a cura di), *Diritto dell'Unione Europea. Parte speciale*, pp. 217 ss., spec. p. 232.

⁷ Sentenza *Schnitzer*, cit., punto 32

⁸ V. sentenze 5 ottobre 1994, TV10, causa C-23/93, C-23/93, Raccolta, pp. I-4795 e ss., punto 15 sentenza 12 settembre 2006 *Cadbury Schweppes e Cadbury Schweppes Overseas*, Causa C-196/04. Raccolta, p. I-07995, punto 37. In dottrina, *ex multis*, v. M. GESTRI, *Abuso del diritto e frode alla legge nell'ordinamento comunitario*, Milano, 2003; S. M. CARBONE, *Brevi riflessioni sull'abuso del diritto comunitario: commercio internazionale ed esercizio delle libertà individuali*, in *Diritto del commercio internazionale*, 2011, pp. 67 ss. .

dell'art. 29. Secondo il Parere 1/2008⁹, nel caso in cui la sede di un'impresa responsabile del trattamento dei dati si trovi al di fuori del territorio SEE ed al trattamento partecipino stabilimenti situati nel territorio di uno Stato membro, si realizza «l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile» secondo la giurisprudenza della Corte di giustizia; mentre nessun rilievo assume la sua forma giuridica (ufficio locale, filiale dotata di personalità giuridica o agenzia affidata a terzi). Il significato del trattamento effettuato «nel contesto delle attività» di uno stabilimento in uno Stato membro si collega ad un suo ruolo rilevante, quale ad esempio la responsabilità delle relazioni con gli utenti del motore di ricerca in una data giurisdizione; la vendita di pubblicità mirata ai suoi abitanti; l'adempimento delle decisioni giudiziarie e/o le risposte alle richieste delle competenti autorità di contrasto di uno Stato membro.

Il successivo Parere n. 8/2010 sul diritto applicabile¹⁰ afferma che l'ambito di applicazione territoriale della normativa nazionale di attuazione della direttiva 95/46 dipendono dal luogo di stabilimento del responsabile del trattamento. Non sono criteri determinanti né la cittadinanza o il luogo di residenza abituale dell'interessato né l'ubicazione fisica dei dati personali¹¹. Infatti, la direttiva 95/46 prevede un vasto campo di applicazione per garantire che gli individui non siano privati della tutela prevista¹² e, al contempo, impedire l'elusione della legge. L'esistenza di uno stabilimento si collega con la nozione di controllo, in quanto l'elemento decisivo per qualificare uno stabilimento è «l'esercizio effettivo e reale di attività mediante un'organizzazione stabile» nel contesto delle quali sono trattati i dati personali. La formulazione del preambolo della direttiva riprende chiaramente il «centro di attività stabile» della giurisprudenza della Corte di giustizia che implica «la presenza permanente di mezzi umani e tecnici necessari per determinate prestazioni di servizi»¹³. La nozione di «contesto

⁹ WP 148, Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca adottato il 4 aprile 2008.

¹⁰ WP 179 Parere sul diritto applicabile, adottato il 16 dicembre 2010

¹¹ WP 179, Parere n. 8/2010, cit., pag. 10

¹² Il considerando 19 della direttiva indica che «lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile; [e] che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo». V anche Considerando 20 in cui si dichiara che «nell'ipotesi in cui il responsabile del trattamento sia stabilito in un paese terzo i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto».

¹³ Sentenze 4 luglio 1985, *Bergholz*, causa 168/84, Racc. 1985, p. 2251, punto 14 e 7

di attività» non implica che la legge applicabile sia quella dello Stato membro in cui è stabilito il responsabile del trattamento, ma quella del paese in cui uno *stabilimento* del responsabile del trattamento svolge *attività correlate al trattamento di dati*. Tale nozione dovrebbe tenere conto di alcuni criteri: il livello di partecipazione di ciascuno stabilimento alle attività nel cui contesto sono trattati i dati personali; la natura di trattamento dei dati personali dei diversi stabilimenti; il livello di partecipazione di ciascuno stabilimento alle attività di trattamento dei dati personali.

Quanto al secondo criterio relativo alla presenza sul territorio di ‘strumenti’ che sono adoperati per il trattamento dei dati (art.4, par. 1, lett. c) della direttiva 95/46), il Gruppo sostiene una tesi che non appare condivisibile. Malgrado la sua formulazione concepita in un’epoca in cui le attività on-line erano assai ridotte, tale criterio dovrebbe applicarsi quando il responsabile del trattamento ha stabilimenti nell’UE, ma le sue attività sono senza rapporto con il trattamento di dati personali¹⁴. Una tesi che sembra superata e contraddetta dall’evoluzione normativa e giurisprudenziale in corso che tende ad annullare del tutto il secondo criterio in parola. Peraltro, l’interpretazione del Gruppo di lavoro del termine ‘strumento’ («equipment»)¹⁵ appare particolarmente estensiva. Vi rientrerebbero svariate tipologie di dispositivi: oggetti che consentono materialmente di raccogliere dati personali (ad esempio il personal computer dell’utente); software che, una volta installati, permettono la fornitura del servizio, quali cookies e apps. Il Gruppo di lavoro ha proposto che nella futura legislazione venga elaborato un «approccio orientato ai destinatari del servizio» quando i responsabili del trattamento non sono stabiliti nell’Unione¹⁶. Dovrebbe trattarsi di un’attività mirata, basata sull’effettivo collegamento con uno specifico Stato membro dell’Unione, quali ad esempio servizi esplicitamente mirati a persone residenti attraverso la presentazione di informazioni nelle lingue dell’Unione; la fornitura di servizi o prodotti negli Stati membri dell’Unione; l’accessibilità ad un servizio subordinata all’uso di una carta di credito dell’Unione; l’invio di pubblicità nella lingua dell’utente o per prodotti e servizi disponibili nell’Unione. Il Gruppo

maggio 1998, *Lease Plan Luxembourg / Stato belga*, causa C-390/96, Raccolta, p. 2553.

¹⁴ V., in particolare, Gruppo di lavoro Articolo 29, parere n. 8/2010, pag. 22

¹⁵ Il Gruppo di lavoro sottolinea inoltre che il termine «equipment» (‘strumenti’) utilizzato nella versione inglese della direttiva è eccessivamente ristretto, in quanto le altre versioni linguistiche adoperano termini più simili all’inglese «means» (‘mezzi’), termine che coprirebbe anche dispositivi immateriali come i cookies, Gruppo di lavoro Articolo 29, parere n. 8/2010, pag. 10, pagg. 23 e 24).

¹⁶ Gruppo di lavoro Articolo 29, parere n. 8/2010, pp. 24 e 31.

di lavoro osserva che questo criterio è già usato nel settore della tutela dei consumatori e la sua estensione al settore della protezione dei dati favorirebbe la coerenza e la certezza giuridica.

4. Le richieste del giudice del rinvio e la posizione dell'Avvocato generale

Al fine di determinare le condizioni per l'applicabilità del diritto nazionale nel caso di specie¹⁷, il giudice del rinvio aveva richiesto l'interpretazione pregiudiziale dell'art. 4 della Direttiva 95/46, in particolare del criterio relativo al trattamento effettuato «nel contesto delle attività di stabilimento» (par. 1, lett. a))¹⁸ e del criterio consistente nel «ricorso a strumenti situati nel territorio di detto Stato membro» (*ivi*, lett. c))¹⁹.

Il giudice del rinvio, riprendendo il parere del WG Art. 29 avanza tre condizioni alternative per la qualificazione di un trattamento-dati nel «contesto delle attività» di stabilimento ai sensi della direttiva 95/46: *a*) il gestore di un motore di ricerca apre in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca e l'attività della quale si dirige agli abitanti di tale Stato; *b*) la società madre designa una filiale situata in tale Stato membro come suo rappresentante e responsabile del trattamento di due file specifici contenenti i dati dei clienti che hanno stipulato contratti con detta società per la fornitura di servizi pubblicitari; *c*) la succursale o la

¹⁷ Nell'ipotesi di uno stabilimento del responsabile del trattamento stabilito in più Stati membri, ciascuno di tali stabilimenti dovrà osservare gli obblighi previsti dalle rispettive disposizioni nazionali (così l'art. 4, c. 1, lett. a).

¹⁸ Vale la pena di riportare per intero il testo del primo par., lett. a) dell'art. 4: «Diritto nazionale applicabile. 1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali: *a*) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile (...).»

¹⁹ Quando, pur non essendovi stabilito, il responsabile impieghi, ai fini del trattamento, strumenti (automatizzati o non) situati nel territorio di uno Stato membro, salva l'ipotesi di mero transito (art. 4, c. 1, lett. c). Nell'ambito del presente lavoro può essere trascurata l'ipotesi piuttosto remota che il diritto nazionale trovi applicazione quando, pur non essendo il responsabile stabilito in uno Stato membro, sia comunque soggetto alla disciplina ivi vigente in orza del diritto pubblico internazionale (art. 4, c. 1, lett. b). Si tratta dell'ipotesi di consolati, ecc.

filiale stabilita in uno Stato membro trasmette alla società madre, avente sede al di fuori dell'Unione, i reclami e le ingiunzioni che le vengono presentati tanto dalle persone interessate quanto dalle autorità competenti per il rispetto del diritto alla protezione dei dati personali, anche quando tale collaborazione abbia carattere volontario²⁰. In effetti, nella sentenza in commento, viene presa in considerazione solo la prima delle tre fattispecie in quanto ritenuta in sé decisiva per l'affermazione del diritto applicabile, così da escludere la necessità di approfondire la rilevanza giuridica delle successive fattispecie prospettate dal giudice del rinvio.

L'Avvocato generale esclude in primo luogo la legittimità della 'creazione' giurisprudenziale di un criterio quale «il centro di gravità del conflitto» non previsto dal diritto secondario dell'Unione sulla base esclusiva dell'ampia tutela dei dati personali prevista dall'art. 8 della Carta dei diritti. Il diritto primario non può determinare l'applicazione della disciplina nello Stato membro in cui si trovi il cittadino dell'Unione senza base alcuna nel diritto secondario. Più in particolare, non è infatti legittimo sulla base di una disposizione della Carta, determinare un ampliamento delle competenze e dell'ambito di applicazione del diritto dell'Unione²¹.

Quanto al criterio relativo allo stabilimento, l'Avvocato generale sottolinea che, il tenore della norma dell'art. 4, lett. a) della direttiva 95/46 non si riferisce ad un trattamento di dati personali effettuato dallo stesso stabilimento interessato, bensì soltanto «nel contesto delle attività» di quest'ultimo. In ogni caso, tale formulazione non può ricevere un'interpretazione restrittiva alla luce del diritto alla vita privata con riguardo al trattamento dei dati personali proclamato dalla Carta dei diritti fondamentali. L'argomento decisivo per un'interpretazione teleologica della norma in parola appare invece la «modalità di business» dei motori di ricerca, nella misura in cui lo stabilimento risulta collegato a un servizio personalizzato di vendita pubblicitaria mirato ai residenti di uno Stato membro. Perciò, il trattamento di dati personali è da considerarsi realizzato nel contesto dallo stabilimento di un responsabile del trattamento, se opera come strumento per «personalizzare e indirizzare la comunicazione commerciale» ai cittadini di uno Stato membro, quand'anche l'indicizzazione dei dati personali sia effettuata fuori dall'Unione.

²⁰ Par. 45 AG.

²¹ Ai sensi del suo articolo 51, paragrafo 2, la Carta non estende l'ambito di applicazione del diritto dell'Unione al di là delle competenze dell'Unione né introduce competenze nuove o compiti nuovi per l'Unione o modifica le competenze e i compiti definiti nei trattati.

5. *L'interpretazione della Corte di Giustizia*

All'inizio della analisi, la Corte rileva alcune caratteristiche dell'organizzazione e delle modalità di svolgimento delle attività (localizzazione degli stabilimenti, «modello di business», divisione dei compiti fra società madre e filiali, ecc)²². La Corte nota che la società madre indicizza i siti web a livello globale e che le informazioni raccolte vengono memorizzate in server dei quali non è resa pubblica l'ubicazione. Anche qualora la qualificazione dell'indicizzazione da parte del motore di ricerca come trattamento dati fosse oggetto di discussione, la Corte ricorda che Google svolge parallela attività di comunicazione pubblicitaria (in corrispondenza della digitazione dei termini da parte degli utenti nelle loro ricerche)²³ tramite le proprie filiali nazionali che provvedono alla gestione delle vendite di spazi pubblicitari. In sostanza, le filiali intra-Ue operano quale agente commerciale del Gruppo Google in ciascuno Stato membro dell'Unione.

Pertanto, seguendo le indicazioni dell'Avvocato generale, la Corte di giustizia afferma l'ambito di applicazione territoriale del diritto nazionale di attuazione della Direttiva 95/46 qualora il gestore di un motore di ricerca stabilito in uno Stato terzo apra in uno Stato membro una filiale per la promozione e alla vendita di comunicazione commerciale diretta ai residenti in quello Stato membro. In proposito, la Corte osserva che Google Spain costituisce una filiale di Google Inc. nel territorio spagnolo e, pertanto, uno 'stabilimento' ai sensi della direttiva; respinge invece la rilevanza giuridica dell'argomentazione secondo cui il trattamento di dati personali da parte di Google Search non sarebbe effettuato nel contesto delle attività di tale stabilimento in Spagna.

Le due finalità di ricerca e pubblicità del motore di ricerca sono pertanto da considerare inscindibili e, così, le relative attività realizzate nel contesto delle attività di stabilimento delle filiali nazionali del Gruppo Google. Quando i dati vengono trattati per le esigenze di un motore di ricerca gestito da un'impresa situata in uno Stato terzo — ma che dispone di uno stabilimento in uno Stato membro — il trattamento è da considerare come effettuato «nel contesto delle attività» della filiale²⁴.

²² Si tratta della prima questione esaminata nella sentenza, v. paragrafi 42-61.

²³ Collocati nella colonna a sinistra dello schermo ma sembra anche con altri favoritismi nell'ordine di apparizione nella lista dei risultati.

²⁴ Alla luce delle considerazioni di cui sopra, occorre rispondere alla prima questione, lettera a), dichiarando che l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel terri-

Quest'ultima ha il compito di assicurare, nello Stato membro in questione, la promozione e la vendita degli spazi pubblicitari proposti sul motore di ricerca al fine di rendere redditizio il servizio offerto (*pay per click*). Non è determinante stabilire se concretamente le singole filiali concorrano all'indicizzazione che può invece essere effettuata e oggetto di archiviazione al di fuori dell'Unione o in un luogo non reso pubblico. Le filiali nazionali sono invece da considerare responsabili del trattamento dei dati per il loro ruolo nell'attività di comunicazione commerciale²⁵, ove si consideri specialmente il posizionamento ovvero la visualizzazione contestuale dei link pubblicitari²⁶.

A rafforzamento della tesi, la Corte²⁷ afferma che nelle circostanze in cui operano i motori di ricerca, non sarebbe legittimo che il trattamento di dati personali venga sottratto agli obblighi e alle garanzie previsti dalla direttiva 95/46, pregiudicandone l'effetto utile e la tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche in una materia come quella del diritto al rispetto della loro vita privata, con riguardo al trattamento dei dati personali.

Secondo il dispositivo della sentenza Google Spain, lo stabilimento in uno Stato membro di un'impresa stabilita fuori dall'Unione ha un ruolo determinante per la definizione del criterio di applicabilità territoriale se implicato un servizio di vendita di pubblicità mirata agli abitanti di tale Stato membro.

torio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro. 61. Tenuto conto della soluzione data alla prima questione, lettera a), non vi è luogo a rispondere alla prima questione, lettere da b) a d).

²⁵ Punti 55 e 56 della sentenza: «Infatti, in circostanze del genere, le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio e che tale motore è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività».

²⁶ Punto 57: «la visualizzazione stessa di dati personali su una pagina di risultati di una ricerca costituisce un trattamento di dati personali. Orbene, poiché la suddetta visualizzazione di risultati è accompagnata, sulla stessa pagina, da quella di pubblicità correlate ai termini di ricerca, è giocoforza constatare che il trattamento di dati personali in questione viene effettuato nel contesto dell'attività pubblicitaria e commerciale dello stabilimento del responsabile del trattamento nel territorio di uno Stato membro, nella fattispecie il territorio spagnolo».

²⁷ Punto 58.

6. La proposta di regolamento della Commissione sulla tutela dei dati personali

Il processo normativa di creazione e rafforzamento del mercato unico si muove nella direzione di effettuare una revisione delle direttive di prima generazione con nuovi regolamenti, come accade nel settore della protezione dei dati personali, ma anche nel settore delle comunicazioni elettroniche²⁸.

Il Consiglio e il Parlamento europeo sembrano orientati ad accettare la proposta della Commissione sui criteri per l'applicabilità delle norme del futuro regolamento²⁹. Tre proposte di ‘considerando’ del regolamento in via di adozione illustrano l'impostazione del nuovo strumento normativo. Il primo criterio, esplicitato nella proposta di ‘considerando’ n. 19, è concordante con l'interpretazione della Corte nella sentenza *Google Spain* secondo cui qualsiasi trattamento effettuato nell'ambito delle «attività di uno stabilimento» deve essere conforme al nuovo regolamento, senza che sia rilevante dove si svolga il trattamento di dati personali (all'interno dell'Unione o al di fuori).

Il secondo, nella proposta di ‘considerando’ n. 20, afferma l'applicabilità del nuovo regolamento al «trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono legate all'offerta di beni o servizi a dette persone indipendentemente dal fatto che vi sia un pagamento o no». Si precisa che l'esistenza di un'offerta di beni o servizi e l'intenzione di «concludere affari» con residenti nell'Unione non sarà ricostruibile esclusivamente sulla base di elementi indiziari alquanto neutrali e non specificamente caratterizzanti (semplice accessibilità di un sito Internet, di un indirizzo di posta elettronica, di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il responsabile del trattamento è stabilito). Maggiore rilevanza dovranno

²⁸ COM(2013) 627, Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure riguardanti il mercato unico europeo delle comunicazioni elettroniche e per realizzare un continente connesso, recante modifica delle direttive 2002/20/CE, 2002/21/CE e 2002/22/CE e dei regolamenti (CE) n. 1211/2009 e (UE) n. 531/2012; cui *Adde* Risoluzione legislativa del Parlamento europeo del 3 aprile 2014 in prima lettura nell'ambito della procedura legislativa ordinaria.

²⁹ Consiglio UE Doc. 6762/1/14 Rev 1, 28 febbraio 2014, Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), Prima lettura, Dibattito orientativo su talune questioni.

assumere fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, e/o la menzione di clienti o utenti residenti nell'Unione. Il terzo, contenuta nel 'considerando' n. 21, afferma in modo del tutto innovativo l'applicabilità del nuovo regolamento ai residenti nell'Unione ad opera di un'impresa non-stabilito nell'Unione quando sia riferito al «controllo del loro comportamento all'interno dell'Unione». Questo criterio di collegamento si riferisce a «tecniche volte alla profilazione dell'utente, in particolare per prendere decisioni che li riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali».

La nuova impostazione è contenuta nella proposta della Commissione di art. 3 del Regolamento³⁰. La novità più rilevante sarà l'introduzione di un ulteriore criterio di applicazione che si articola in due sotto-criteri: *a)* l'offerta di beni o la prestazione di servizi ai residenti nell'Unione; *b)* il controllo del loro comportamento» (art. 3, par. 2). Mentre la prima fattispecie di «servizi indirizzati a livello trasfrontaliero» manifesta la convergenza della disciplina dei dati personali verso quella già in vigore per altri diritti online (diritti della personalità, marchio e, parzialmente copyright); la seconda ipotesi -relativa al «controllo dei comportamenti» degli utenti da parte degli operatori non-stabiliti nell'Unione-richiederà un complesso approfondimento proprio a partire dal concetto di profilazione dei dati personali.

7. Il criterio di collegamento dell'attività diretta nella scelta della legge applicabile al contratto del consumatore e il criterio del «centro di interessi» del consumatore per la determinazione della competenza giurisdizionale

Un inquadramento nel diritto secondario dell'Unione in vigore per altri diritti on line, merita il criterio di collegamento di «un'attività diretta» al pubblico di un altro Stato membro cui fa riferimento la proposta

³⁰ Articolo 3, Campo di applicazione territoriale: 1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione. 2. Il presente regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: *a)* l'offerta di beni o la prestazione di servizi ai suddetti residenti nell'Unione, oppure *b)* il controllo del loro comportamento.(...).

di regolamento sulla protezione dei dati personali, di cui abbiamo appena accennato. In alcune sentenze, la Corte di giustizia ha privilegiato il criterio che l'attività di un sito fosse diretta rispettivamente al pubblico dell'Unione europea o al pubblico di uno Stato membro³¹. Tale criterio (*intention to target*) è stato applicato anche ad attività transfrontaliere anche non on-line con la specificazione che deve rivelare «l'intenzione del suo autore di rivolgersi alle persone che si trovano in tale territorio³²».

In materia di competenza giurisdizionale e di conflitto di leggi, tale criterio che collega l'applicabilità territoriale al pubblico cui l'attività si rivolge (*intention to target*) è prevista dai regolamenti Bruxelles I³³ e «Bruxelles I-bis»³⁴, nonché dal regolamento Roma I (art. 6)³⁵. La Corte di giustizia nella sentenza *Pammer e Hotel Alpenhof*³⁶ ha indicato i requisiti che un sito *web* deve soddisfare affinché le attività esercitate dal com-

³¹ Sentenze *L'Oreal* e a. cit. (punto 65) in materia di marchi nazionali e comunitari e 18 ottobre 2012, *Football Dataco Ltd e a.*, causa C-173/11, punto 39), sulla violazione del diritto sui generis su una banca dati.

³² Sentenza 21 giugno 2012, causa C-5/11, non ancora pubblicata in Raccolta, punto 21; cit. (punto 27) sulla violazione del diritto esclusivo di distribuzione di un autore (operazioni di vendita transfrontaliera di mobili protetti in uno Stato membro dal diritto d'autore).

³³ Regolamento (CE) n. 44/2001 del Consiglio, del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GUCE L 12, pag. 1), e sentenze del 7 dicembre 2010, *Pammer e Hotel Alpenhof* (C-585/08 e C-144/09, Racc. pag. I-12527), nonché 19 aprile 2013, Causa C-523/10, non ancora pubblicata, in Raccolta.

³⁴ L'art. 15, par. 1, lett. c) stabilisce che la competenza in materia di contratti conclusi dai consumatori sussiste: (...) c) in tutti gli altri casi, qualora il contratto sia stato concluso con una persona le cui attività commerciali o professionali si svolgono nello Stato membro in cui è domiciliato il consumatore o sono dirette, con qualsiasi mezzo, verso tale Stato membro o verso una pluralità di Stati che comprende tale Stato membro, purché il contratto rientri nell'ambito di dette attività.» La formulazione dell'art. 17, par. 1, lett. c) del Regolamento «Bruxelles I-bis» è identica a quella del regolamento «Bruxelles I» salvo che per la condizione aggiuntiva che «il contratto rientri nell'ambito di dette attività», v. Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio del 12 dicembre 2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, GUUE L 351, 20.12.2012, pp. 1 ss.

³⁵ Art. 6 Contratti conclusi da consumatori: «(...) è disciplinato dalla legge del paese nel quale il consumatore ha la residenza abituale, a condizione che il professionista (...) b) diriga tali attività, con qualsiasi mezzo, verso tale paese o vari paesi tra cui quest'ultimo» v. regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I), GUUE L 177 del 4.7.2008, pp. 6 ss.

³⁶ Sentenza 7 dicembre 2010, cause riunite C-585/08 e C-144/09, *Pammer e Hotel Alpenhof*, cit., punti 67 e 68.

mercante possano essere considerate 'dirette verso' lo Stato membro del consumatore. La pubblicità on line deve essere attentamente qualificata come attività transfrontaliera diretta verso il consumatore domiciliato in un altro Stato membro, ad esclusione delle due opposte situazioni: da un lato, la semplice accessibilità di un sito negli Stati membri; dall'altro, l'esistenza di indizi evidenti che l'attività è rivolta «in modo sostanziale», verso lo Stato membro di domicilio del consumatore³⁷. All'interno dell'arco fra queste due fattispecie, la Corte indica numerosi criteri esemplificativi di tale proiezione transfrontaliera del professionista on line³⁸. Nella sentenza *Emrek*, la Corte ha poi precisato la necessità di un nesso di causalità tra il mezzo (il sito Web) impiegato per dirigere l'attività commerciale verso lo Stato membro di domicilio del consumatore e la conclusione del contratto³⁹.

Infine, ci sembra rilevante segnalare che, nella prospettiva della determinazione della competenza giurisdizionale, la Corte di giustizia abbia avuto modo di specificare l'importanza del «concetto di centro di interessi» del consumatore precisando che corrisponde, in via generale, alla sua residenza abituale. Nella Sentenza *eDate Advertising e Martinez*⁴⁰, la Corte

³⁷ Ivi., punti 69 e 82.

³⁸ A tal proposito, la Corte fornisce dunque una lista non esaustiva, vale a dire: i) la natura internazionale dell'attività, quali talune attività turistiche; ii) la menzione di recapiti telefonici con indicazione del prefisso internazionale; iii) l'utilizzazione della denominazione di un sito di primo livello diverso da quello dello Stato membro in cui il commerciante è stabilito; iv) l'utilizzazione di denominazioni di siti di primo livello neutri quali «.com» o «.eu»; v) l'indicazione di itinerari a partire da uno o più Stati membri verso il luogo della prestazione dei servizi, nonché vi) la menzione di una clientela internazionale composta da clienti domiciliati in Stati membri diversi, in particolare mediante la presentazione di testimonianze provenienti dai clienti medesimi. Qualora inoltre il sito Internet permetta al consumatore di usare lingue e monete diverse, tale impiego può assumere rilevanza e costituire un indizio finalizzato a tale valutazione (a contrario tali elementi non possono essere considerati pertinenti nel caso in cui lingua e moneta impiegate siano quelle abitualmente utilizzate nello Stato membro a partire dal quale il commerciante esercita la propria attività). Ivi, *Pammer e Hotel Alpenhof*, cit., punti 83 e 84.

³⁹ Sentenza 17 ottobre 2013, causa C-218/12, *Emrek*, non ancora pubblicata in *Raccolta*, punto 29.

⁴⁰ Sentenza della Corte (grande sezione) del 25 ottobre 2011, *eDate Advertising GmbH e Martinez*, cit. Per un commento, v. C.I. NAGY, *The Word is a Dangerous Weapon: Jurisdiction, Applicable Law and Personality Rights in EU law - Missed and New Opportunities*, in *Journal of Private International LAW*, 2012, pp. 251 ss.; T. HARTLEY, *Cross-Border Privacy Injunctions: The EU Dimension*, in *The Law Quarterly Review*, 2012, pp. 197 ss.; M. WINKLER, *Giurisdizione e diritto applicabile agli illeciti via web: nuovi importanti chiarimenti dalla Corte di giustizia*, in *Responsabilità civile e previdenza*, 2012, pp. 806 ss.; G. GIOIA, *Sulla distribuzione della competenza internazio-*

ha interpretato il regolamento Bruxelles I (art. 5, n. 3), istitutivo di un foro speciale in materia di illeciti civili dolosi o colposi, nelle controversie su violazioni di diritti della personalità a causa della pubblicazione on-line di contenuti diffamatori. Nella sua argomentazione, la Corte ha osservato che a seguito della diffusione universale di Internet, da un lato, si accresce, la gravità delle violazioni dei diritti della personalità; dall’altro, diventa estremamente difficile individuare i luoghi di concretizzazione del danno. È però evidente che l’impatto di un’informazione sui diritti della personalità può essere meglio apprezzato dal giudice del luogo in cui la vittima ha il proprio «centro di interessi», corrispondente per lo più alla residenza. Pertanto la Corte ha individuato tale giudice come quello competente per la totalità dei danni causati sul territorio dell’Unione europea⁴¹.

8. Cenni alla giurisprudenza sulla responsabilità degli ISP ‘attivi’ e ‘passivi’

Mentre nella sentenza Google Spain la Corte ha statuito che l’attività del motore di ricerca è sicuramente qualificabile come attività di trattamento-dati, in altri casi ha preferito lasciare al giudice del rinvio pregiudiziale la qualificazione in concreto dell’attività dell’Isp nel contesto del procedimento principale.

Vale pertanto la pena di ricordare lo stato dell’arte della giurisprudenza della Corte sulla responsabilità degli operatori ‘intermediari’ (ISP) che forniscono le tecnologie e le attività di supporto per il mercato online. La Corte di giustizia prosegue nel percorso di individuazione e qualificazione della responsabilità di quei soggetti che non si limitano ad un’attività di intermediazione passiva ma partecipano in modo qualificato all’attività dei *content provider*. È certamente il caso dell’attività dei motori di ricerca, ma anche dei prestatori di servizi di aggregatori dei contenuti, secondo i modelli di eBay, Facebook e You tube.

La Corte di giustizia fornisce un contributo creativo allo sviluppo del regime giuridico di tali prestatori di servizi in relazione alle trasformazioni tecnologiche ed economiche che hanno uno specifico impatto soprattutto nel settore del commercio elettronico la cui disciplina è prevedibile non sarà oggetto di riforma a breve⁴². Il regime normativo dell’Unione resta

nale nelle liti da diffamazione tramite internet, in *Riv. dir. proc.*, 2012, pp. 1317 ss.

⁴¹ Ivi, punti 48 e 49.

⁴² SEC(2011) 1641 final, 11.1.2012, Online services, including e-commerce, in the Single Market, Accompanying the document COM(2011) 942 final, Un quadro coeren-

così articolato in relazione al ruolo e alle funzioni delle diverse categorie degli operatori coinvolti, secondo la classificazione della direttiva sul commercio elettronico⁴³: fornitori di accesso alle reti di comunicazioni elettroniche (*access provider*); prestatori di servizi che si limitano a svolgere una funzione di diffusione passiva dei contenuti (operatori di servizi tecnici di *mere conduit*, *caching* e *hosting*) ex articoli 12, 13 e 14 della direttiva 2000/31. Quest'ultimi sono ritenuti, in generale, eleggibili ad una deroga di responsabilità: il criterio dell'imputazione della colpa è ritenuto dal legislatore dell'Unione un criterio ragionevole per evitare un controllo delle attività dal costo eccessivo (divieto di controllo generalizzato) e il rischio di censura dei materiali dei *content provider* potenzialmente lesivi di diritti altrui. In siffatto contesto non ha tardato ad emergere la categoria dei prestatori di servizi che *non* si limitano a svolgere una funzione di diffusione passiva dei contenuti ma interferiscono attivamente nell'elaborazione e/o presentazione finale degli stessi (ISP attivi).

Pertanto, la responsabilità di ISP quali i motori di ricerca, i *social network* e gli «aggregatori di contenuti generati dagli utenti» non appare definibile *una tantum*, ma solo sulla base del grado di interferenza concretamente esercitato nell'attività dei soggetti-terzi (*content provider*) direttamente responsabili delle violazioni. Nella prospettiva della tutela dei beni digitali veicolati su Internet, tali soggetti sono tenuti in misura crescente, tra l'altro, al rispetto di principi di responsabilità civile nonché a responsabilità specifiche per la tutela del marchio e del diritto d'autore⁴⁴. Nella sua giurisprudenza, la Corte ha iniziato a delimitare e circoscrivere le caratteristiche di un ISP 'puramente passivo' eleggibile, ai sensi della direttiva sul commercio elettronico, ad una deroga nella responsabilità civile delle sue

te per rafforzare la fiducia nel mercato unico digitale del commercio.

⁴³ Direttiva 2000/31/CE, cit. Sentenza L'Oréal e a.

⁴⁴ Sul tema della responsabilità civile degli ISP si vedano: V. ZENO-ZENCOVICH, *I rapporti tra responsabilità civile e responsabilità penale nelle comunicazioni su Internet (riflessioni preliminari)*, in *Dir. Inf.* 1999, pp. 1050 ss.; T. PASQUINO, *Servizi telematici e criteri di responsabilità*, Milano, 2003; F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003; S. SICA, *Le responsabilità civili*, in E. TOSI (a cura di), *Commercio elettronico e servizi della società dell'informazione*, Milano, 2003, pp. 267 ss.; M. GAMBINI, *Le responsabilità civili dell'Internet service provider*, Napoli, 2006; E. TOSI, *Diritto privato dell'informatica e di Internet. I beni - I contratti - Le responsabilità*, Milano, 2006; M. DE CATA, *La responsabilità civile dell'internet service provider*, Milano, 2010; A. MANTELEO, *La responsabilità online: il contratto nella prospettiva dell'impresa*, in *Dir. Inf.*, 2010, pp. 405 ss.; E. TOSI, *La responsabilità civile per fatto illecito degli Internet Service Provider e dei motori di ricerca a margine di recenti casi «Google Suggest» per errata programmazione dei Software di ricerca e «Yahoo Italia!» per link illecito in violazione dei diritti di proprietà intellettuale*, in *Riv. Dir. Ind.*, 2012, pp. 44 ss.

attività rispetto a quella dei suoi *content provider*. Certamente, l’attività di un motori di ricerca, come Google, è qualificato fra gli operatori qualificati come ISP attivi ai quali non spetta l’esonero di responsabilità prevista dalla direttiva sul commercio elettronico. Non a caso nella sentenza *Google Spain* viene citata ‘per analogia’ la precedente sentenza *L’Oréal*⁴⁵ in relazione all’operatore eBay in base allo svolgimento di un ruolo attivo di conoscenza e controllo dei dati relativi alle aste⁴⁶. Il parametro rilevante diventa il contributo offerto dall’ISP nella presentazione finale e promozione del contenuto digitale diffuso *online*.

La Corte ha fornito alcune precisazioni riguardo alla responsabilità del gestore di un mercato su Internet che, pur non essendo l’utilizzatore dei marchi quando si limita a consentire ai propri clienti di riprodurre segni corrispondenti a marchi, è tuttavia responsabile laddove svolga un ruolo attivo atto a conferirgli una conoscenza o un controllo dei dati relativi a dette offerte. Il gestore non può quindi essere esonerato da qualsiasi responsabilità qualora assista i propri clienti nell’ottimizzare la presentazione delle offerte o nel promuovere le medesime. Egli non può essere a maggior ragione esonerato qualora sia stato al corrente di fatti o

⁴⁵ Sentenza 12 luglio 2011, *L’Oréal SA e altri c. eBay International AG e altri*, cit., punto 62: «(...) Una situazione del genere vanificherebbe l’effetto utile di tali norme» e punto 63: «(...) sarebbe pregiudicata l’efficacia di tali norme qualora l’uso, in un’offerta in vendita o in una pubblicità su Internet destinata a consumatori che si trovano nell’Unione, di un segno identico o simile a un marchio registrato nell’Unione fosse sottratto all’applicazione di tali norme per il solo fatto che il terzo all’origine di detta offerta o pubblicità sia stabilito in uno Stato terzo, che il server del sito Internet da lui utilizzato si trovi in tale Stato o ancora che il prodotto oggetto di detta offerta o pubblicità si trovi in uno Stato terzo.».

⁴⁶ J. VAN HOBOKEN, *Search engine freedom: on the implications of the right to freedom of expression for the legal governance of web search engines*, Alphen aan den Rijn, 2012; P. SAVOLA, *The ultimate copyright shopping opportunity: jurisdiction and choice of law in website blocking injunctions*, in *IIC: international review of industrial property and competition law*, 2014, pp. 287 ss.; A. DALY, *Dominating Search: Google Before the Law* (April 25, 2014), in R. KONIG, M. RASCH (eds), *Reflections on Web Search*, Amsterdam, 2014, 86-104 (<http://ssrn.com/abstract=2429129>); J. CORNTHWAITE, *Say it with flowers: the judgment of the Court of Justice of the European Union in «Interflora v Marks & Spencer»*, in *European Intellectual Property Review*, 2012, pp. 127-132; C. MORCOM, *Trade marks and the Internet: where are we now?*, in *European Intellectual Property Review* 2012, pp. 40 ss.; G. PSAROUDAKIS, *In search of the trade mark functions: keyword advertising in European law*, in *European Intellectual Property Review*, 2012, pp. 33 ss.; A. WAISMAN, M. HEVIA, *Theoretical foundations of search engine liability*, in *IIC: international review of industrial property and competition law*, 2011, pp. 785 ss.; J. CORNTHWAITE, *To key or not to key?: The judgment of the European Court of Justice in the «Google France AdWords» case*, in *European Intellectual Property Review*, 2010, pp. 352 ss.

circostanze in base ai quali un operatore diligente dovrebbe constatare l'illiceità delle offerte in vendita online e non abbia prontamente agito per rimuovere i dati di cui trattasi o renderne l'accesso impossibile.

Tra le numerose sentenze sul sistema di posizionamento della pubblicità sul motore di ricerca Google⁴⁷, è sufficiente ricordare la sentenza *Google France SARL e Google Inc./Louis Vuitton Malletier SA* a.⁴⁸, in cui la Corte ha dovuto risolvere difficili questioni sull'uso on line del marchio, interpretando le disposizioni del regolamento n. 40/94 (art. 9, n. 1) e della direttiva 89/104/CEE (art. 5, nn. 1 e 2)⁴⁹. La Corte è stata al riguardo interrogata in merito alla responsabilità di un operatore quale la società Google per i dati dei suoi clienti memorizzati sul proprio server. Le questioni di responsabilità sono disciplinate dal diritto nazionale. Per quanto attiene alla questione se il servizio di posizionamento su Internet costituisca un servizio della società dell'informazione (consistente nel memorizzare informazioni fornite dall'inserzionista) se, pertanto, il prestatore di tale servizio goda di una limitazione di responsabilità, la Corte ha rilevato che spetta al giudice del rinvio valutare se il ruolo svolto da tale prestatore sia neutro, in quanto il suo comportamento è meramente tecnico, automatico e passivo, comportante una mancanza di conoscenza o di controllo dei dati che esso memorizza. Infatti, secondo la Corte, qualora risulti che il prestatore di servizi di posizionamento non ha svolto un ruolo attivo, non può essere ritenuto responsabile per i dati che egli ha memorizzato su richiesta di un inserzionista, salvo che, essendo venuto a conoscenza della natura illecita di tali dati o di attività di tale inserzionista, egli abbia omesso di rimuovere prontamente tali dati o disabilitarne l'accesso. In senso inverso, nei confronti di ISP 'passivo', la Corte di Giustizia

⁴⁷ Sul sistema di pubblicità tramite parole chiave, v. le sentenze 23 marzo 2010, *Google France* e *Google*, cause riunite C-236/08 a C-238/08, Raccolta, p. I-02417, punti 22 e 23; 25 marzo 2010, *BergSpechte*, causa C-278/08, Raccolta, p. I-2517, punti da 5 a 7; 8 luglio 2010, causa C-558/08, *Portakabin* e *Portakabin*, Raccolta, p. I-6963, punti da 8 a 10; 22 settembre 2011, *Interflora Inc.* e *Interflora British Unit*, causa C-323/09, Raccolta p. I-08625, punti da 9 a 13.

⁴⁸ Sentenza 23 marzo 2010, cause riunite da C-236/08 a C-238/08, *Google France SARL* e *Google Inc./Louis Vuitton Malletier SA*, cit., punti 106-120

⁴⁹ Regolamento (CE) n. 40/94 del Consiglio, del 20 dicembre 1993, sul marchio comunitario, GUCE L 11, 14/01/1994, p. 1 ss.; Prima direttiva 89/104/CEE del Consiglio, del 21 dicembre 1988, sul ravvicinamento delle legislazioni degli Stati membri in materia di marchi d'impresa, GUCE 1989, L 40, pp. 1 ss.

nelle sentenze *Scarlet c. Sabam*⁵⁰ e *Scarlet c. Netlog*⁵¹ ha ritenuto incompatibili con la normativa comunitaria, l'imposizione di sistemi di filtraggio dei contenuti digitali a tutela dei diritti di proprietà intellettuale di tutte le comunicazioni elettroniche in transito per i suoi servizi, in particolare mediante programmi «peer-to-peer», se rivolti indistintamente a tutta la sua clientela; a titolo preventivo; a spese esclusive dell'ISP e senza limiti nel tempo, idoneo ad identificare nella rete di tale fornitore la circolazione di file contenenti un'opera musicale, cinematografica o audiovisiva rispetto alla quale il richiedente affermi di vantare diritti di proprietà intellettuale, onde bloccare il trasferimento di file il cui scambio pregiudichi il diritto d'autore.

Abstract

The article examines critically the notion of «established activity» as used in the Google Spain decision in the light of the consolidated ECJ jurisprudence on the existence of a «stable organization» and the effect it may have in the future also to determine the applicable law and the competent jurisdiction.

⁵⁰ Sentenza 24 novembre 2011, *Scarlet c. SABAM*, causa C-70/10, Raccolta, p. I-11959. Per un commento, v. M. RANTOU, *The growing tension between copyright and personal data protection on an online environment: The position of Internet Service Providers according to the European Court of Justice*, in *European Journal of Law and Technology*, 2012, Issue 2, pp. 1 ss.; C. D'ANGELO, *Corte europea di giustizia, 24 novembre 2011, C-70/10*, in *Europa e diritto privato*, 2012, pp. 663 ss.; P. SAMMARCO, *Alla ricerca del giusto equilibrio da parte della Corte di giustizia UE nel confronto tra diritti fondamentali nei casi di impiego i sistemi tecnici di filtraggio*, in *Dir.Inf.*, 2012 pp. 297 ss.

⁵¹ Sentenza 16 febbraio 2012, *SABAM c. Netlog NV*, causa C-360/10, non ancora pubblicata in Raccolta. Per un commento, v. M. BELLIA, G. A. M. BELLOMO, M. MAZZONCINI, *La responsabilità civile dell'Internet Service Provider per violazioni del diritto d'autore*, in *Il diritto industriale*, 2012 pp. 346 ss.; C. D'ANGELO, *Corte europea di giustizia, 24 novembre 2011, C-70/10*, in *Europa e diritto privato*, 2012, pp. 663 ss. Su entrambe le sentenze, v. M. COLANGELO, *Internet e sistemi di filtraggio tra enforcement del diritto d'autore e tutela dei diritti fondamentali: un commento ai casi Scarlet e Netlog*, in *La nuova giurisprudenza civile commentata*, 2012, pp. 580 ss.

Profili internazionale-privatistici della responsabilità del gestore di un motore di ricerca per il trattamento dei dati personali

SOMMARIO: 1. Introduzione - 2. I fatti davanti alla Corte di giustizia - 3. I criteri di applicabilità della direttiva 95/46 quando il responsabile del trattamento è stabilito in uno o più Stati membri: la lett. a) dell'art. 4, par. 1 - 4. I criteri di collegamento nei casi nei quali il responsabile del trattamento non è stabilito nel territorio di uno Stato membro: la lett. c) dell'art. 4, par. 1 - 5. La natura giuridica dell'art. 4 - 6. I vizi argomentativi delle conclusioni dell'avvocato generale e della sentenza della Corte di giustizia - 7. L'art. 3 della proposta di regolamento di riforma della direttiva. In particolare: il «*targeting test*»

1. Introduzione

La questione internazionale-privatistica è al centro della direttiva 95/46/CE, che definisce il quadro generale del trattamento dei dati personali e della libertà di circolazione di tali dati tra Stati membri dell'Unione europea e membri dell'Accordo relativo allo spazio economico europeo¹.

Emanata sulla base dell'art. 100A Tr. CE, relativo al ravvicinamento delle legislazioni nel quadro del mercato interno (ora art. 114 TFUE),

¹ Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in *G.U.*, L 281 del 23 novembre 1995, pp. 31 ss., successivamente modificata dall'all. II al regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio del 29 settembre 2003 recante adeguamento alla decisione n. 1999/468/CE del Consiglio delle disposizioni relative ai comitati che assistono la Commissione nell'esercizio delle sue competenze di esecuzione previste negli atti soggetti alla procedura prevista all'art. 251 Tr. CE, *ibid.*, L 284 del 31 ottobre 2003, pp. 1 ss. La direttiva è stata inserita nell'Accordo relativo allo «spazio economico europeo» («SEE/EEA») con l'art. 2 della decisione del Comitato misto SEE n. 83/1999 del 25 giugno 1999, che modifica il protocollo n. 37 e l'all. XI (servizi di telecomunicazione) dell'Accordo «SEE» (*ibid.*, L 296 del 23 novembre 2000, p. 41 ss.). Inoltre, la direttiva è stata inclusa nell'all. B dell'Accordo del 26 ottobre del 2004 tra l'UE, la CE e la Confederazione svizzera (che non è Stato contraente dell'Accordo SEE, ma è parte dell'«Associazione europea di libero scambio», «AELS/EFTA»), riguardante l'associazione di quest'ultima all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen (*ibid.*, L 53 del 27 febbraio 2008, pp. 52 ss.).

la direttiva persegue l'obiettivo di garantire la libertà di circolazione dei dati personali attraverso l'armonizzazione delle legislazioni nazionali sulla tutela delle persone fisiche rispetto al trattamento di questi dati. Infatti, una volta eliminato il «divario nei livelli di tutela dei diritti e delle libertà» individuali garantiti negli Stati membri relativamente al trattamento di dati personali» (considerando 7 e 8), data la protezione equivalente derivante dal ravvicinamento delle legislazioni nazionali, «gli Stati membri non [avrebbero potuto] più ostacolare la libera circolazione tra loro di dati personali per ragioni inerenti alla tutela dei diritti e delle libertà delle persone fisiche, segnatamente del diritto alla vita privata» (considerando 9)². Il testo della direttiva evidenzia chiaramente l'intento del legislatore di attribuire una funzione strumentale al diritto alla protezione dei dati personali rispetto alla libertà di circolazione di tali dati nel mercato interno: «gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela... dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali» (art. 1, par. 2 e 1). I criteri di applicabilità territoriale delle misure legislative nazionali di trasposizione della direttiva, stabiliti dall'art. 4, svolgono una funzione cruciale nel perseguimento del principale obiettivo che il legislatore si era prefisso con la direttiva, cioè la garanzia della libertà di circolazione dei dati personali nel mercato interno³. L'art. 4 è una (complicata) versione della clausola «mercato interno», che sancisce una sorta di principio dello Stato di origine: vista la mancanza di disposizioni vincolanti di armonizzazione a livello dell'Unione, al fine di garantire la libertà di circolazione dei dati personali nel mercato interno, la direttiva obbliga il legislatore nazionale a provvedere affinché il responsabile del trattamento dei dati personali stabilito sul territorio di uno Stato membro rispetti le misure nazionali di recepimento della direttiva in vigore nello Stato di stabilimento (mentre il responsabile non stabilito rispetterà le disposizioni nazionali in vigore nello Stato membro nel quale si trova la strumentazione che utilizza, a determinate condizioni, per il trattamento dei dati personali)⁴.

Tuttavia, la direttiva 95/46/CE persegue anche l'obiettivo di garantire la tutela dei diritti delle persone fisiche con riguardo al trattamento dei

² Cfr. le conclusioni dell'avv. gen. Tizzano presentate il 19 settembre 2002, nel caso *Bodil Lindqvist*, in causa C-101/01, in *Racc.*, 2003, pp. I-12971 ss., par. 39.

³ Cfr. la prima Relazione della Commissione sull'applicazione della direttiva sulla tutela dei dati cit., p. 17, par. 4.4.1.

⁴ V. *infra*, rispettivamente, par. 3 e 4.

dati personali. L'entrata in vigore della direttiva ha segnato in particolare l'avvio di un percorso volto al riconoscimento nella Comunità europea del diritto soggettivo alla protezione dei dati personali come diritto fondamentale dell'individuo. Se l'art. 286 Tr. CE, inserito dal Trattato di Amsterdam (*ex art.* 213B), si è limitato a estendere l'applicazione della direttiva alle istituzioni e agli organi comunitari e a prevedere la nascita del «Garante europeo della protezione dei dati»⁵, l'art. 16 TFUE, recuperando l'art. I-51 Tr. Cost., ha introdotto il diritto fondamentale di «ogni persona» alla protezione dei dati che la riguardano⁶. L'art. 8 della Carta dei diritti fondamentali dell'Unione europea, alla quale il Trattato di Lisbona ha attribuito lo stesso valore giuridico dei trattati (art. 6, par. 1 TUE), ha riaffermato l'inviolabilità di questo diritto, anche se la Corte di giustizia ha ritenuto che non si tratti di una prerogativa assoluta né incondizionata, ma di una garanzia che può essere limitata in considerazione della sua «funzione sociale»⁷. Le limitazioni che possono essere legittimamente apposte al diritto fondamentale alla protezione dei dati personali sancito dall'art. 8 della Carta corrispondono a quelle tollerate per il diritto alla riservatezza, tutelato nel quadro del rispetto della vita privata e familiare *ex art.* 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali («CEDU»). In applicazione dell'art. 6, par. 3 TUE, che ha attribuito efficacia vincolante all'art. 8 CEDU quale parte dei principi generali dell'UE⁸, e dell'art. 52, par. 3

⁵ Il Garante europeo è stato istituito dall'art. 41 del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in *G.U.*, L 8 del 12 gennaio 2001, pp. 1 ss.

⁶ Questa norma costituisce attualmente la base giuridica generale per le misure dell'Unione relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e alla libertà di circolazione di tali dati: cfr. P. PIRODDI, *Art. 16 TFUE*, in F. POCAR, M.C. ARUFFI (a cura di), *Commentario breve ai trattati dell'Unione europea*, 2° ed., Padova, 2014, pp. 189 ss. Una base giuridica speciale destinata al settore della politica estera e di sicurezza comune è prevista dall'art. 39 TUE: v. A. LANG, *Art. 39 TUE*, *ibid.*, p. 123.

⁷ Corte di giustizia, 12 giugno 2003, *Schmidberger*, in causa C-112/00, in *Racc.*, 2003, pp. I-5659 ss., par. 80 e giurisprudenza *ivi cit.*; 9 novembre 2010, *Volker und Markus Schecke*, nelle cause riunite C-92/09 e C-93/09, *ibid.*, 2010, pp. I-11063 ss., par. 48. Cfr. anche Corte di giustizia, 6 novembre 2003, *Bodil Lindqvist*, in causa C-101/01, *ibid.*, 2003, pp. I-12971 ss., par. 82-90; 16 dicembre 2008, *Satamedia*, in causa C-73/07, *ibid.*, 2008, pp. I-9831 ss., par. 50-62.

⁸ In specifica relazione al diritto alla protezione dei dati personali, cfr. Corte di giustizia, 9 novembre 2010, *Volker und Markus Schecke cit.*, par. 47 ss., nella quale la Corte mette

della Carta, il diritto alla protezione dei dati personali deve essere interpretato anche in conformità alla giurisprudenza della Corte europea dei diritti dell'uomo sull'art. 8 CEDU. In realtà, il diritto alla protezione dei dati personali si è emancipato dal diritto alla riservatezza delle persone fisiche ex art. 8 CEDU già con la convenzione del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale, firmata a Strasburgo il 28 gennaio 1981⁹; tuttavia, su questo strumento, aperto anche all'adesione di Stati non membri del Consiglio d'Europa, la Corte europea dei diritti dell'uomo non esercita giurisdizione. Via via che il diritto alla protezione dei dati personali è si rafforzato nell'Unione europea¹⁰, acquistando la natura di diritto

in stretta relazione l'art. 8 CEDU e gli artt. 7 e 8 della Carta attraverso il riferimento all'art. 52, n. 3 e all'art. 53 della stessa Carta, creando in tal modo un anello di congiunzione tra la CEDU il sistema di tutela dei diritti fondamentali proprio dell'ordinamento giuridico dell'UE.

⁹ Convenzione STCE n. 108, entrata internazionalmente in vigore il 1° ottobre 1985, per l'Italia il 1° luglio 1997 e per la CE il 15 giugno 1999 (v. *Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede*, adottati dal Comitato dei Ministri a Strasburgo il 15 giugno 1999. Cfr. anche il Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STCE n. 181), firmato a Strasburgo l'8 novembre 2001, entrato in vigore il 1° luglio 2004. Sulla convenzione cfr., per tutti, F. HENKE, *Die Datenschutzkonvention des Europarates*, Frankfurt a.M-Bern-New York, 1986, pp. 5 ss. Sulla genesi del diritto alla protezione dei dati personali dal diritto alla riservatezza e, in definitiva, del diritto al rispetto della vita privata, cfr. P. PIRODDI, *Art. 8 Carta dei diritti fondamentali dell'Unione europea*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve cit.*, pp. 1682 ss.

¹⁰ Cfr., ad es., la differenza che intercorre tra l'affermazione della Corte di giustizia, nella sentenza 20 maggio 2003, *Österreichischer Rundfunk*, nelle cause riunite C-465/00, C-138/01 e C-139/01, in *Racc.*, pp. I-4989 ss. par. 70: «La stessa direttiva 95/46, pur avendo come obiettivo principale quello di garantire la libera circolazione dei dati personali, prevede, al suo art. 1, n. 1, che '[g]li Stati membri garantiscono (...) la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali'; e l'ammissione di segno contrario che si rinviene della sentenza 7 maggio 2009, *Rijkeboer*, in causa C-553/07, *ibid.*, 2009, pp. I-3889 ss., par. 46: «Ai sensi dell'art. 1 della direttiva, il suo obiettivo è tutelare le libertà e i diritti fondamentali delle persone fisiche, in particolare la loro vita privata, con riguardo al trattamento dei dati personali, e permettere, in tal modo, la libera circolazione dei dati tra gli Stati membri». In crescendo, cfr. altresì la categorica dichiarazione secondo la quale «L'art. 1 della direttiva 95/46 prescrive agli Stati membri di garantire la tutela delle libertà e dei diritti fondamentali delle persone fisiche, in particolare della loro vita privata, con riguardo al trattamento dei dati personali», di cui alla sentenza del 16 dicembre 2008, *Huber*, in causa C-524/06, *ibid.*, 2011, p. I-9705, par. 47, ripetuta

fondamentale dell'individuo, l'interpretazione dell'art. 4 della direttiva si è modificata in conseguenza di questa evoluzione: l'art. 4 non è più stato visto come una clausola «mercato interno», così come era stata concepita in origine dal legislatore, ma come una vera e propria norma di diritto internazionale privato, alla quale è stata attribuita la funzione di determinare la legge applicabile al trattamento dei dati personali nell'Unione, delimitando così i confini nello spazio del diritto fondamentale alla protezione dei dati personali tutelato dall'ordinamento europeo. Nel contempo, l'esigenza di estendere la protezione individuale che consegue al carattere fondamentale del diritto alla tutela dei dati personali, che ha indotto ad escludere qualsiasi interpretazione riduttiva delle disposizioni sostanziali della direttiva, ha spinto anche a dilatare oltremisura i criteri di applicabilità territoriale contenuti nella direttiva. Questo ha condotto ad una prassi di applicazione esorbitante della legislazione nazionale degli Stati membri, che invece di contribuire a promuovere la libertà di circolazione dei dati personali nel mercato interno, ha creato un ostacolo alla libertà di prestazione dei servizi nel settore dell'*information technology*, rischiando di isolare il mercato interno in settori fondamentali del trasferimento internazionale di dati, e di ridurre lo spazio economico europeo ad un'area puramente domestica o regionale. Il «disperato bisogno» del settore delle tecnologie dell'informazione di criteri di collegamento più adeguati per la definizione della legge applicabile al trattamento dei dati personali è stata una tra le principali ragioni che hanno convinto la Commissione ad intraprendere la revisione della direttiva¹¹. Nel pacchetto di riforma del quadro

nella sentenza 24 novembre 2011, *ASNEF e FECMD*, nelle cause riunite C-468/10 e C-469/10, *ibid.*, 2011, pp. I-12181 ss., par. 25. Sotto questo aspetto, è evidente che l'interpretazione della direttiva non è stata conforme al principio di effettività, poiché non ha realizzato tutte le finalità perseguite dall'atto: sul principio di effettività cfr., da ultimo, Corte di giustizia, 6 maggio 2010, *Club Hotel Loutraki*, nelle cause riunite C-145/08 e C-149/08, *ibid.*, 2010, p. I-4165 ss., par. 74 e giurisprudenza ivi cit. Tuttavia, v., da ultimo, la dichiarazione equilibrata della Corte di giustizia, nella sentenza 7 novembre 2013, *IPI*, in causa C-473/12, non ancora pubbl., par. 28: «Risulta dai considerando 3, 8 e 10 della direttiva 95/46 che il legislatore dell'Unione ha inteso facilitare la libera circolazione dei dati personali ravvicinando le legislazioni degli Stati membri pur salvaguardando i diritti fondamentali della persona, in particolare il diritto alla tutela della vita privata, e garantendo un elevato grado di tutela nell'Unione».

¹¹ Cfr. le conclusioni dello studio sponsorizzato dalla Commissione *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments. Final Report*, 20 gennaio 2010, in http://ec.europa.eu/justice/policies/privacy/docs/studi es/new_privacy_challenges/final_report_en .pdf, p. 26 [consultato 30/09/2014], riprese sia da «THE ARTICLE 29 WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA»

generale della protezione dei dati personali nell'Unione europea presentato dalla Commissione, la proposta di regolamento, destinato a sostituire la direttiva¹², contiene criteri di collegamento di natura indiscutibilmente internazionalprivatistica, che svolgono la funzione di determinare la legge applicabile al trattamento dei dati personali da parte degli Stati membri dell'Unione europea e dell'Accordo sullo spazio economico europeo. L'iter legislativo della proposta è stato tuttavia rallentato da forti contrasti tra istituzioni e Stati membri¹³, che si sono accentuati dopo la prima lettura del Parlamento europeo: infatti, pur approvando il testo proposto dalla Commissione, il Parlamento ha apposto emendamenti tali da sbilanciare il nuovo regolamento verso la protezione sostanziale di un diritto individuale, più che verso il buon funzionamento del mercato interno¹⁴. La

(d'ora in avanti «THE ARTICLE 29 WORKING PARTY»: v. *infra*, nota 31), *Opinion 8/2010 on Applicable Law*, adottata il 16 dicembre 2010, 0836-02/10/EN, WP 179, p. 5, sia dalla comunicazione della Commissione *Un approccio globale alla protezione dei dati personali nell'Unione europea*, del 4 novembre 2010, COM(2010)609 def., p. 11. Cfr. anche THE EUROPEAN DATA PROTECTION SUPERVISOR (v. *supra*, nota 5), *Opinion on the Communication from the Commission «A comprehensive approach on personal data protection in the European Union»*, in [http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_\(2\)_15_th_rt_2011.pdf](http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_(2)_15_th_rt_2011.pdf), p. 5 [consultato 30/09/2014]. V. altresì, già in questo senso, la prima Relazione della Commissione sull'applicazione della direttiva sulla tutela dei dati cit., p. 17.

¹² Cfr. la proposta relativa ad un regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, COM(2012)11 def. - 2012/0011(COD). Gli altri atti che fanno parte del «pacchetto» sono la comunicazione della Commissione *Salvaguardare la privacy in un mondo interconnesso - Un quadro europeo della protezione dei dati per il XXI secolo*, COM(2012)9 def.; una proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (COM(2012)10 def. - 2012/0010 (COD)), destinata a sostituire la decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (in *G.U.*, L 350 del 30 dicembre 2008, pp. 60 ss.); e infine una relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, basata sull'art. 29, par. 2, della decisione quadro 2008/977/ GAI (doc. COM(2012)12, con l'allegato SEC(2012) 75 def.), relativa all'attuazione di questa decisione negli Stati membri.

¹³ Cfr. N. VANDYSTADT, *Open Clash Pits Reding against Council over Data Protection*, in *Europolitics*, n° 4768/2013 del 9 dicembre 2013, p. 9.

¹⁴ Risoluzione legislativa del Parlamento eur. del 12 marzo 2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati

Commissione, nella relazione di accompagnamento alla proposta originaria, aveva tuttavia sottolineato che la regolamentazione del trattamento dei dati personali costituisce un pilastro centrale del sostegno alla crescita dei servizi relativi alle tecnologie dell'informazione nel mercato interno, e che la riforma della direttiva costituisce una delle componenti chiave del piano d'azione per l'attuazione dell'«Agenda digitale europea» e della stessa strategia «Europa 2020»¹⁵. Il difficile esercizio di equilibrio richiesto al legislatore per contemperare le due anime della disciplina del trattamento dei dati personali appare quindi ancora lontano dall'esser risolto. In attesa della posizione comune del Consiglio¹⁶, inoltre, i conflitti sono stati rinfocolati dalla sentenza della Corte di giustizia nel caso *Digital Rights Ireland*, che ha annullato la direttiva 2006/24/CE sulla conservazione dei dati, ritenendo il livello di salvaguardia dei dati personali insufficiente a soddisfare i requisiti posti dalla Carta dei diritti fondamentali dell'Unione europea¹⁷. In questa fase delicatissima, la Corte di giustizia è chiamata, nel caso *Google Spain SL e Google Inc.*¹⁸, a interpretare per la prima volta,

(regolamento generale sulla protezione dei dati) (COM(2012)0011 - C7- 0025/2012 - 2012/0011(COD)) (Procedura legislativa ordinaria: prima lettura) P7_TA(2014)0212 del 12 marzo 2014.

¹⁵ Cfr. Commissione, doc. COM(2012)11 def. - 2012/0011(COD) cit., p. 2, par. 1, in riferimento all Comunicazione della Commissione *Un'agenda digitale europea*, COM(2010) 245 def. del 19 maggio 2010; Comunicazione della Commissione *EUROPA 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva*, COM(2010)2020 def. del 3 marzo 2010.

¹⁶ Il 6 giugno 2014 si è riunito a Lussemburgo il Consiglio GAI, durante il quale i ministri hanno raggiunto l'orientamento generale parziale sul capo quinto della proposta di regolamento. Inoltre, si è tenuto un dibattito orientativo circa il meccanismo «one-stop shop»: cfr. nota della Presidenza del Consiglio al Coreper/Consiglio, doc. 10139/14, 2012/0011(COD) del 26 maggio 2014. Cfr. anche le conclusioni del Consiglio di Lussemburgo del 7 ottobre 2013, n. 14525/13, che supporta l'«one-stop shop» e i principi di prossimità e coerenza.

¹⁷ Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland Ltd*, nelle cause riunite C-293/12 e C-594/12, non ancora pubbl., che ha dichiarato invalida e annullato la direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (in *G.U.*, L 105 del 13 aprile 2006, pp. 54 ss.), perché consente un'ingerenza ingiustificata, di vasta portata, e di particolare gravità nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale, garantiti dagli artt. 7 e 8 della Carta, e perché eccede i limiti imposti dal rispetto del principio di proporzionalità alla luce dell'art. 52, par. 1 della stessa Carta.

¹⁸ Corte di giustizia (Grande sezione), 13 maggio 2014, in causa C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, in Appendice a questo Volume. Le conclusioni dell'avv. gen. N. JÄÄSKINEN presentate il 25

dopo quasi vent'anni dall'entrata in vigore della direttiva, i criteri di applicabilità territoriale delle misure nazionali di recepimento degli Stati membri stabiliti dall'art. 4 della direttiva. La Corte conferma la prassi relativa all'interpretazione estensiva delle condizioni di applicazione delle legislazioni nazionali di trasposizione della direttiva; così facendo, tuttavia, evidenzia inevitabilmente tutte le contraddizioni insite nei criteri di applicabilità della direttiva, segnando così la condanna dell'art. 4. Per altro verso, la sentenza, che richiama in più punti il contenuto internazionalprivatistico della proposta della Commissione relativa al nuovo regolamento, ancora *in fieri*, contribuisce significativamente a delineare i futuri contorni delle disposizioni di diritto internazionale privato che determineranno la legge applicabile alla protezione dei dati personali per gli Stati membri dell'Unione europea.

2. I fatti davanti alla Corte di Giustizia

Il rinvio pregiudiziale è stato sollevato dall'Audiencia Nacional, organo giurisdizionale specializzato, con sede a Madrid, nel quadro di una controversia che ha contrapposto le società Google Spain SL e Google Inc. a un cittadino spagnolo, domiciliato in Spagna, Mario Costeja González, e all'Agencia Española de Protección de Datos («AEPD»), l'autorità garante per la tutela dei dati personali della Spagna. Mario Costeja González aveva verificato che, inserendo il suo nome sul motore di ricerca Google, tra i risultati indicizzati compariva un link verso alcune pagine della versione elettronica del quotidiano «La Vanguardia» dell'anno 1998 sulle quali figurava una pubblicità legale per la vendita all'asta di un immobile di proprietà dello stesso Costeja González, a seguito di un pignoramento effettuato per la riscossione coattiva di crediti previdenziali. Egli aveva

giugno 2013, sono anch'esse in Appendice. Per alcuni commenti alle conclusioni dell'avv. gen. cfr. P.-A. DUBOIS, *Search Engines and Data Protection: A Welcome Practical Approach by the Advocate General*, in *Computer and Telecommunications Law Rev.*, 2013, pp. 206 ss.; S. ALICH, L. SAGALOV, *Konzernverbundene Unternehmen ohne Datenverarbeitung als Anknüpfungspunkt umfassender datenschutzrechtlicher Verantwortlichkeit?*, in *Computer und Recht*, 2013, pp. 783 ss.; A. STADLER, R. TOMAN, *Limited Liability of Internet Search Engine Service Providers for Data Protection of Personal Data Displayed on Source Web Pages*, in *Eur. Law Rep.*, 2013, pp. 286 ss.; B. VAN ALSENOY, A. KUCZERAWY, J. AUSLOOS, *Search Engines after Google Spain: internet@liberty or privacy@peril*, ICRI Working Paper, n. 15/ 2013, 6th September 2013, in [https:// www.law.kuleuven.be/icri/ssrn.php](https://www.law.kuleuven.be/icri/ssrn.php) [consultato 30/09/2014].

quindi presentato un reclamo all'AEPD contro «La Vanguardia Ediciones» SL, e contro Google Spain SL e Google Inc. Quest'ultima è la società madre del gruppo Google, con sede in California, e gestisce direttamente il motore di ricerca, nelle differenti versioni disponibili nelle diverse lingue nazionali.

Google Spain SL, con sede sociale a Madrid, è una delle filiali, con personalità giuridica autonoma, costituite da Google Inc. in vari Paesi europei ed extraeuropei, che operano in qualità di agenti commerciali e rappresentanti locali del gruppo per la promozione, lo sviluppo e la vendita a terzi di prodotti e di servizi di pubblicità online, in particolare di spazi pubblicitari generati sul sito dello stesso motore di ricerca. Google permette infatti, attraverso la piattaforma *AdWords*, di far apparire tra i risultati di una ricerca anche link pubblicitari a pagamento, mediante la selezione di una o più parole chiave, qualora tale o tali parole coincidano con quella o quelle contenute nella richiesta indirizzata al motore di ricerca (*keyword advertising*). In aggiunta a questo, Google offre anche un servizio di sponsorizzazione, affiliando, tramite il programma *AdSense*, siti esterni che presentano determinati requisiti.

Le controllate locali di Google svolgono sostanzialmente un'attività di intermediazione diretta ad inserzionisti locali (che acquistano annunci pubblicitari tramite *AdWords*) e editori terzi (che ospitano la pubblicità contestuale *AdSense* sui propri siti), remunerandosi con una percentuale sull'investimento pubblicitario, senza ingerirsi direttamente nelle attività relative al motore di ricerca. Infatti, come risulta dai fatti di causa esposti dal giudice del rinvio, Google Spain risulta responsabile soltanto del trattamento dei dati personali degli inserzionisti, perlopiù imprese stabilite in Spagna, che concludono contratti di servizi pubblicitari con Google Inc. Non è noto, tuttavia, se nella pagina dei risultati della ricerca effettuata dal Costeja González con il suo nome comparissero effettivamente risultati sponsorizzati, che si attivano soltanto a condizione che la parola chiave attraverso la quale è effettuata la ricerca sia stata effettivamente acquistata da un inserzionista locale a scopi pubblicitari. L'AEPD respingeva il reclamo di Costeja González nella parte in cui era diretto contro l'editore del quotidiano, che nell'ordinamento spagnolo è obbligato a pubblicare gli annunci relativi alla pubblicità legale dei procedimenti esecutivi immobiliari. Il reclamo veniva invece accolto nella parte diretta contro Google Spain e Google Inc., alle quali l'AEPD ordinava di adottare le misure necessarie per rimuovere dagli indici del motore di ricerca i link verso le pagine contenenti i dati personali obsoleti del reclamante, e di impedire

in futuro l'accesso a tali pagine tramite il motore di ricerca. Adita da Google Inc. e da Google Spain, in sede di ricorso contro il provvedimento dell'AEPD, l'Audiencia Nacional riteneva tuttavia che sussistessero dubbi sull'interpretazione della direttiva, e chiedeva alla Corte di giustizia di pronunciarsi in via pregiudiziale¹⁹. Quattro dei quesiti sottoposti alla Corte riguardavano esclusivamente l'interpretazione dell'art. 4 della direttiva, che stabilisce i criteri di applicabilità territoriale delle misure legislative nazionali che recepiscono la direttiva stessa nell'ordinamento nazionale degli Stati membri.

3. I criteri di applicabilità della direttiva 95/46 quando il responsabile del trattamento è stabilito in uno o più Stati membri: la lett. a) dell'art. 4, par. 1

In base alla lett. a) dell'art. 4, par. 1, quando il responsabile del trattamento è stabilito nel territorio di uno Stato membro²⁰, e il trattamento di dati personali è effettuato «nel contesto delle attività» dello stabilimento del responsabile del trattamento, è applicabile la legislazione nazionale di trasposizione dello Stato membro nel quale è situato tale stabilimento²¹. L'applicazione della lett. a) dell'art. 4, par. 1 richiede quindi innanzitutto

¹⁹ Vedi il riassunto dei fatti nella sentenza cit., par. 14 ss., e nelle conclusioni dell'avv. gen. JÄÄSKINEN cit., par. 18 ss.

²⁰ Quando invece il responsabile del trattamento è stabilito nel territorio di più Stati membri, esso dovrà «adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile» (art. 4, par. 1, lett. a, *in fine*), secondo un criterio di applicazione distributiva delle legislazioni nazionali che ha suscitato parecchie critiche per le difficoltà di applicazione da parte degli operatori, ai quali è addossato un gravoso onere di *compliance*, tenuto conto della mancanza di uniformità con la quale diversi Stati membri hanno dato concretamente attuazione alla direttiva: cfr. la prima Relazione della Commissione sull'applicazione della direttiva sulla tutela dei dati cit., p. 17, par. 4.4.1. V. anche THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 5. In via di deroga, la lett. b) dell'art. 4, par. 1 considera stabilito in uno Stato membro il responsabile del trattamento che sia stabilito in uno Stato terzo assoggettato alla legislazione nazionale di tale Stato membro in forza del diritto internazionale pubblico: è il caso cosiddetto «diplomatico», che estende l'applicazione della legislazione nazionale di trasposizione della direttiva anche alle rappresentanze diplomatiche e consolari all'estero di un determinato Stato membro, o alle navi, nei casi nei quali il diritto internazionale le consideri sottoposte alla sovranità dello Stato della bandiera: cfr. U. DAMMAN, S. SIMITIS, *EG-Datenschutzrichtlinie: Kommentar*, Baden-Baden, 1997, p. 30.

²¹ Cfr. il considerando 18 della direttiva.

l'identificazione del «responsabile del trattamento», cioè del soggetto che, da solo o insieme ad altri, determina «le finalità e i mezzi del trattamento di dati personali», *ex art. 2, lett. d*)²², e, in secondo luogo, esige l'individuazione dello «stabilimento» del responsabile del trattamento nel territorio di uno Stato membro. In base al considerando 19 della direttiva, il fattore decisivo per qualificare uno «stabilimento» ai fini dell'art. 4 è «l'esercizio effettivo e reale dell'attività [economica] mediante un'organizzazione stabile». Questa definizione si riferisce chiaramente alla giurisprudenza della Corte di giustizia relativa all'«organizzazione stabile» nel quadro del diritto di stabilimento²³ e della libertà di prestazione di servizi²⁴ dell'epoca nella quale era stata emanata la direttiva, e riflette anche l'interpretazione della Corte del «centro di attività stabile» in tema di imposizione fiscale indiretta²⁵. Inoltre, nel considerando 19 può riscontrarsi altresì l'influenza

²² Si noti che il soggetto definito «responsabile del trattamento» dall'art. 2, lett. d della direttiva («la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali»), è stato definito «titolare» del trattamento all'art. 4, lett. f) della misura italiana di attuazione della direttiva, il d. lgs. 30 giugno 2003, n. 196, succ. modif., Codice in materia di protezione dei dati personali («la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso «il profilo della sicurezza»). Per questo Codice è invece «responsabile» del trattamento «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali» (art. 4, lett. g) Codice), che in realtà è il soggetto definito come «incaricato del trattamento» all'art. 2, lett. e) della direttiva («la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento»). L'art. 4, lett. h) del Codice italiano definisce invece «incaricati» del trattamento le «persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile». V. su queste definizioni THE ARTICLE 29 WORKING PARTY, *Opinion 1/2010 on the concepts of «controller» and «processor»*, doc. WP 169 del 16 febbraio 2010, pp. 7 ss.

²³ Cfr. Corte di giustizia, 4 ottobre 1991, in causa C-246/89, *Commissione c. Regno Unito*, in *Racc.*, 1991, pp. I-4585 ss., par. 21; 25 luglio 1991, in causa C-221/89, *Factortame Ltd*, *ibid.*, 1991, pp. I-3905 ss., par. 20. Cfr. anche THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 11.

²⁴ Cfr. Corte di giustizia, 4 dicembre 1986, in causa C-205/84, *Commissione c. Germania*, in *Racc.*, 1986, pp. 3755 ss., par. 21; 20 febbraio 1997, in causa C-260/95, *DFDS*, *ibid.*, 1997, pp. I-1005 ss., par. 29.

²⁵ Corte di Giustizia, 4 luglio 1985, *Berkholz*, in causa 168/84, in *Racc.*, 1985, pp. 2251 ss., par. 18; 2 maggio 1996, *Faaborg- Gelting Linien*, in causa C-231/94, *ibid.*, 1996, p. I-2395, par. 17; 17 luglio 1997, *ARO Lease*, in causa C-190/95, *ibid.*, 1997, pp. I-4383 ss., par. 19; 7 maggio 1998, *Lease Plan Luxembourg*, in causa C-390/96, *ibid.*, 1998, pp.

di una nozione propria dell'ambito dell'imposizione fiscale diretta, e cioè la «stabile organizzazione» (*permanent establishment*), accolta nella *Model Convention with Respect to Taxes on Income and on Capital* dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE)²⁶, che costituisce il criterio fondamentale di attribuzione della potestà impositiva agli Stati ai fini dell'eliminazione delle doppie imposizioni, ed è oggetto di diffusa adesione da parte della pratica internazionale. Il considerando 19 della direttiva precisa che, per determinare lo «stabilimento nel territorio di uno Stato membro» non rileva la forma giuridica attraverso la quale l'impresa del responsabile del trattamento è stabilita. Può trattarsi, dunque, della sede principale, oppure di una filiale dotata di autonoma personalità giuridica, di una semplice succursale o sede secondaria, o di un'agenzia che agisca in qualità di ausiliaria del responsabile del trattamento, o persino di «un semplice ufficio, gestito da personale dipendente dall'impresa, o [da] una persona indipendente, ma incaricata di agire in permanenza per conto dell'impresa alla stessa stregua di un'agenzia²⁷».

Terza e ultima condizione perché uno Stato membro possa applicare la propria misura nazionale di trasposizione ad uno stabilimento del responsabile del trattamento situato nel proprio territorio è che il trattamento dei dati personali sia effettuato «nel contesto delle attività» dello stabilimento. Il requisito del «contesto delle attività» consente di applicare la misura nazionale di trasposizione della direttiva a un responsabile del trattamento che abbia uno stabilimento nel territorio di uno Stato membro, *a prescindere dal luogo nel quale sono effettuate tecnicamente le operazioni di trattamento dei dati personali*, luogo che può anche trovarsi in un altro Stato membro o in uno Stato terzo. Il legislatore ha inteso così evitare il rischio di *forum shopping*, il rischio cioè che l'applicazione della direttiva venga elusa semplicemente spostando il trattamento dei dati personali in uno

I-2553 ss., par. 26.

²⁶ Cfr. Article 5, *Permanent Establishment*, della *Model Convention with Respect to Taxes on Income and on Capital*, adottata il 30 luglio 1963 come *Draft Convention* dall'*Organisation for Economic Co-operation and Development* (OECD). Sul punto, cfr. OECD COMMITTEE ON FISCAL AFFAIRS, *Model Tax Convention on Income and on Capital, Commentary on Article 5*, 8th ed., 2010, Paris; OECD *Model Tax Convention: Revised Proposals Concerning the Interpretation and Application of Article 5 (Permanent Establishment)*, 19th October, 2012 to 31st January, 2013, in <http://www.oecd.org/ctp/treaties/PermanentEstablishment.pdf> [consultato 30/09/2014]. La nozione di «*permanent establishment*» è stata traspota in Italia dall'art. 162 d.P.R. 22 dicembre 1986, n. 917, introdotto dall'art. 1 d.lgs. 12 dicembre 2003, n. 344.

²⁷ Cfr. Corte di giustizia, 20 febbraio 1997, *DFDS* cit., par. 29; 4 dicembre 1986, *Commissione c. Germania* cit., par. 21.

Stato terzo²⁸. Infatti, non è necessario che il trattamento di dati personali venga effettuato «dallo» stabilimento del responsabile del trattamento nel territorio di uno Stato membro, bensì soltanto che venga effettuato «nel contesto delle attività» di questo stabilimento: la legislazione applicabile non è quella dello Stato membro nel quale il responsabile del trattamento è stabilito, ma quella dello Stato membro nel quale *uno stabilimento* del responsabile del trattamento svolge *attività nel contesto delle quali* è effettuato il trattamento dei dati personali²⁹. Quindi, uno Stato membro non potrà applicare la propria misura nazionale di attuazione della direttiva, qualora il responsabile del trattamento abbia uno stabilimento nel proprio territorio che effettui un trattamento di dati personali *nel contesto di attività diverse* da quelle svolte in quello specifico stabilimento³⁰. Secondo l'interpretazione del «Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali» («Gruppo Articolo 29»³¹), qualora uno stabilimento effettui un trattamento di dati personali *nel contesto delle attività che esso stesso svolge*, la legge applicabile è quella dello Stato membro nel quale questo stabilimento è situato. Qualora questo stabilimento effettui trattamenti di dati personali *nel contesto delle attività di un altro stabilimento*, sarà invece applicabile la legge nazionale dello Stato membro nel quale si trova quest'altro stabilimento³².

Questo è un criterio di difficile applicazione pratica, poiché solleva

²⁸ Cfr. CH. KUNER, *Internet Jurisdiction and Data Protection Law: An International Legal Analysis. Part 1*, in *Int'l Journ. Law Inform. Technology*, 2010, pp. 176 ss.; ID., *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, *ibid.*, 2010, pp. 227 ss.; F. RIGAUX, *Libre circulation des données et protection de la vie privée dans l'espace européen*, in J. BASEDOW, U. DROBNIG, K.J. HOPT, H. KÖTZ (Hrsgs.), *Festschrift für Ulrich Drobnig zum siebzigsten Geburtstag*, Tübingen, 1998, pp. 425 ss., e in P. TABATONI (dir.), *La protection de la vie privée dans la société de l'information. L'impact des systèmes électroniques*, t. II, Paris, 2000, pp. 25 ss., a p. 38.

²⁹ Cfr. THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 13: «The notion of «context of activities» does not imply that the applicable law is the law of the Member State where the controller is established, but where an establishment of the controller is involved in activities relating to data processing».

³⁰ Per alcuni esempi, cfr. THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 13; W. KUAN HON, J. HÖRNLE, CH. MILLARD, *Data Protection Jurisdiction and Cloud Computing - When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing. Part 3*, 2011 (updated 09/02/2012), in <http://www.cloudlegal.ccls.qmul.ac.uk/docs/63746.pdf>, pp. 8 ss.

³¹ È un organo indipendente con funzioni consultive, istituito a livello europeo ex art. 29 della direttiva 95/46/CE: per ulteriori approfondimenti, cfr. P. PIRODDI, *Art. 16* cit., p. 191.

³² THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 14.

inevitabilmente la questione del grado di coinvolgimento richiesto allo stabilimento del responsabile del trattamento nelle attività nel contesto delle quali sono trattati i dati personali, coinvolgimento che dipende a sua volta dalla natura delle attività che sono svolte in concreto dallo stabilimento. Il criterio del «contesto delle attività» si presta anche ad anche estendere eccessivamente l'applicabilità delle misure legislative degli Stati membri, poiché si applica anche quando i dati personali trattati non riguardano cittadini o residenti di uno Stato membro³³.

Il criterio del «contesto delle attività» è stato oggetto di un parere esplicativo del «Gruppo Articolo 29», che aveva ipotizzato proprio il caso del gestore di un motore di ricerca, non stabilito in uno Stato membro, che effettui un trattamento di dati personali al di fuori dello spazio economico europeo³⁴. Se il responsabile del trattamento possiede una filiale o una succursale nell'Unione europea, la lett. a) dell'art. 4, par. 1 consente di affermare che il trattamento avviene «nel contesto delle attività» della controllata europea, anche se questa non effettua direttamente alcun trattamento di dati personali, ma semplicemente vende pubblicità in collegamento con queste attività, limitandosi a negoziare con gli imprenditori locali che acquistano annunci pubblicitari. Questa interpretazione è stata avallata dalla nostra Corte di cassazione nel caso *Vivi Down*, relativo al caso un utente italiano che aveva caricato un *file* video sulla piattaforma *Google Video*, operata gratuitamente da Google Inc., come il motore di ricerca. La Cassazione ha ritenuto che il trattamento dei dati personali contenuti nel video, benché effettuato esclusivamente da Google Inc. presso la sua sede negli Stati Uniti, fosse stato svolto «nel contesto delle attività» di Google Italy Srl, la controllata locale costituita da Google Inc. in Italia, sulla sola base del fatto che Google Italy poteva collegare *link* pubblicitari alla pagina del servizio di *hosting video*³⁵.

³³ Cfr., ad es., THE ARTICLE 29 WORKING PARTY, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by non-EU Based Web Sites*, doc. WP 56 del 30 maggio 2002, p. 6; Id., *Opinion 1/2008 on data protection issues related to search engines*, doc. WP 148 del 4 April 2008, pp. 9-10; *Opinion 1/2010 on the concepts of «controller» and «processor»* cit., p. 5; *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, doc. WP 128 del 22 November 2006, par. 2 ss. In dottrina, cfr. U. DAMMANN, S. SIMITIS, *EG-Datenschutzrichtlinie: Kommentar* cit., pp. 127-128.

³⁴ THE ARTICLE 29 WORKING PARTY, *Opinion 1/2008 on data protection issues related to search engines* cit., pp. 9 ss. Cfr. anche, in senso analogo, ID., *Working Document on Determining the International Application of EU Data Protection Law* cit., p. 8.

³⁵ Cass. pen., III sez., 17 dicembre 2013-3 febbraio 2014, n. 5107, in *Foro it.*, 2014,

4. I criteri di collegamento nei casi nei quali il responsabile del trattamento non è stabilito nel territorio dello Stato membro: la lett. c) dell'art. 4, par. 1

Se il responsabile del trattamento non è stabilito nel territorio di uno Stato membro, la lett. a) dell'art. 4, par. 1 non è applicabile. Al «responsabile non stabilito nel territorio della Comunità» si applica esclusivamente la lett. c) dell'art. 4, par. 1. Tuttavia, il «Gruppo Articolo 29» ha evidenziato che tra queste due ipotesi si apre una terza possibilità, per la quale l'art. 4, par. 1 non prevede nulla: è il caso nel quale il responsabile del trattamento è stabilito nel territorio di uno Stato membro, ma il trattamento di dati personali non è effettuato «nel contesto delle attività» svolte da quello stabilimento³⁶: ossia, lo stabilimento del responsabile del trattamento svolge attività che non sono in relazione al trattamento di dati personali. In questo caso, non è applicabile la lett. c), che presuppone che il responsabile del trattamento non sia stabilito nel territorio di uno Stato membro; né è applicabile la lett. a, poiché presuppone non semplicemente l'esistenza di uno stabilimento del responsabile del trattamento in uno Stato membro, ma l'esistenza di uno stabilimento che effettui un trattamento di dati personali *nel contesto delle stesse attività svolte da questo stabilimento*³⁷.

La lett. c) prevede l'applicazione della legislazione nazionale di trasposizione dello Stato membro nel quale sono fisicamente situati gli «

II, cc. 336 ss., nota di F. DI CIOMMO, *Google/Vivi Down, atto finale: l'hosting provider non risponde quale titolare del trattamento dei dati*, *ibid.*, cc. 346 ss., a parziale conforto della sentenza della Corte d'Appello di Milano, sez. I pen., 27 febbraio 2013 e del Trib. Milano, sez. IV pen., 12 aprile 2010, n. 1972, in http://www.giurcost.org/casi_sceltil/Google.pdf, p. 102-103. Cfr. G. SARTOR, M. VIOLA DE AZEVEDO CUNHA, *The Italian Google Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, in *Int'l Journ. Law Inform. Technology*, 2010, pp. 1 ss.; N. DE LUCA, E. TUCCI, *Il caso Google/Vivi Down e la responsabilità dell'internet service provider. Una materia che esige chiarezza*, in *Giur. comm.*, 2011, II, pp. 1215 ss.; O. POLLICINO, *Modeling the Liability of Internet Service Providers: Google vs. Vivi Down. A Constitutional Perspective*, Milano, 2013, pp. 5 ss. Per una decisione di segno contrario, cfr. in vece la decisione del Garante della protezione dei dati personali su ricorso del 3 novembre 2009, <http://www.garanteprivacy.it/garantel/doc.jsp?ID=1687662>.

³⁶ THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 2: «[Article 4(1)c] should apply in those cases where there is no establishment in the EU/EEA which would trigger the application of Article 4(1)a or where the processing is not carried out in the context of such an establishment».

³⁷ Secondo il «Gruppo Articolo 29», in questo caso di vuoto normativo dovrebbe applicarsi la lett. c) dell'art. 4, par. 1: THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., pp. 19, 22.

strumenti, automatizzati o non automatizzati », che sono utilizzati ai fini del trattamento dei dati personali, ad eccezione del caso nel quale questi strumenti siano adoperati «ai soli fini di transito nel territorio» dell'Unione europea³⁸. Nessuna definizione o interpretazione di «strumenti, automatizzati o non automatizzati» è contenuta nel testo della direttiva, né nella relazione di accompagnamento della Commissione. Questa omissione ha causato una grave incertezza applicativa in riferimento a questa disposizione³⁹; tuttavia, quando la direttiva è stata adottata, la nozione di «strumenti» veniva generalmente riferita alle infrastrutture fisiche (*computers, servers, data centres*) che, trovandosi nella disponibilità del responsabile del trattamento (benché non necessariamente nella sua proprietà), potevano essere operate da remoto dallo stabilimento del responsabile del trattamento. Correlativamente, per strumenti «utilizzati ai soli fini di transito nel territorio», il legislatore intendeva escludere soltanto una ristretta categoria di dispositivi: ad esempio, cavi di connessione delle reti di telecomunicazione, *routers, switches* e *bridges*, cioè i nodi che, all'interno di una stessa rete, svolgono direttamente o indirettamente la funzione di instradare i dati verso reti differenti.

Nel corso del tempo, tuttavia, l'intento di ampliare l'ambito di applicazione della direttiva, in considerazione del carattere inviolabile del diritto alla protezione dei dati personali⁴⁰, ha indotto a estendere via via

³⁸ Cfr. il considerando 20 della direttiva.

³⁹ Per un'interpretazione di questo concetto, cfr. THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 20.

⁴⁰ Su questo punto v. specificamente S. RODOTÀ, *Data Protection as a Fundamental Right*, in S. GUTWIRTH *et al.* (eds.), *Reinventing Data Protection?*, Dordrecht-Heidelberg-London-New York, 2009, pp. 77 ss. CH. KUNER, *European Data Protection Law-Corporate Compliance and Regulation*, 3rd ed., Oxford, 2007, pp. 21 ss., sembra concludere che l'art. 4, par. 1, lett. c non è basato su un principio di territorialità, ma su un principio di protezione o persino sulla c.d. «teoria degli effetti». L'A., in riferimento THE ARTICLE 29 WORKING PARTY, *Working Document on Determining the International Application of EU Data Protection Law* cit., p. 7, argomenta che: «The Article 29 Working Party has indicated that the protection of individuals inside the EU is one of the main purposes of Article 4(1)(c), a view which is shared by some commentators [U. DAMMANN, *Internationaler Datenschutz, Recht der Datenverarbeitung*, 2002, p. 73]. Thus, it seems that the function of this provision is largely to protect individuals in the EU, even if it does not fulfill the traditional criteria of protective jurisdiction »; e prosegue: «While seeming to apply the objective territoriality principle, Article 4(1)(c) is focused not on the use of equipment per se, but on preventing data controllers from evading EU rules by relocating outside the EU. Thus, Article 4(1)(c) also focuses on the effect produced in the EU by data processing outside the EU, and the protection of EU citizens, meaning that it can also be viewed as an application of the effects doctrine».

il concetto di «strumenti, automatizzati o non automatizzati», al punto che questo, attualmente, non risponde più a caratteristiche fisiche, ma ad un'istanza puramente virtuale. Si ritiene, ad esempio, anche l'invio di *cookies* da *server* situati al di fuori dello spazio economico europeo a *client* di utenti situati in uno Stato membro corrisponderebbe all'utilizzazione di «strumenti automatizzati» situati nello spazio economico europeo, poiché tali programmi vengono eseguiti dalla macchina dell'utente (ad esempio, dal *browser*). Un punto di vista analogo è stato espresso in riferimento a *scripts*, a *spywares*, a determinati *banners* pubblicitari (*online behavioural advertising*) e ad altri programmi del genere, anch'essi eseguiti dalla macchina dell'utente e non dalla piattaforma *web* del *server* di invio⁴¹.

Anche questa disposizione è stata chiaramente concepita per prevenire casi di *forum shopping* e di elusione della legislazione europea attraverso lo spostamento dello stabilimento che effettua il trattamento nel territorio di Stati dalla legislazione meno restrittiva⁴². Nel contempo, questo criterio è inteso a prevenire il rischio che un responsabile del trattamento non stabilito utilizzi il territorio dello spazio economico europeo per effettuare trattamenti di dati personali non conformi alla direttiva⁴³. Tuttavia, anche la lett. *c* può condurre, interpretata così estensivamente, a situazioni di *regulatory overreaching*, nelle quali la misura nazionale di recepimento della direttiva di uno Stato membro è applicata a situazioni prive di effettivo collegamento con questo Stato⁴⁴. Infatti, benché effettuato attraverso l'utilizzazione di strumenti situati nello spazio economico europeo, il trattamento di dati personali può riguardare dati di persone che non hanno necessariamente né la cittadinanza, né la residenza nel territorio di uno Stato membro⁴⁵.

⁴¹ Cfr. THE ARTICLE 29 WORKING PARTY, *Working Document on Determining the International Application of EU Data Protection Law* cit., p. 11-12; ID., *Opinion 1/2008 on Data Protection Issues Related to Search Engines* cit., p. 11; ID., *Opinion 8/2010 on Applicable Law* cit., p. 23.

⁴² Cfr. U. DAMMANN, S. SIMITIS, *EGDatenschutzrichtlinie: Kommentar* cit., p. 129; C. DE TERWANGNE, S. LOUVEAUX, *Data Protection and Online Networks*, in *Computer Law and Security Report*, 1997, pp. 234 ss., a pp. 238-239; CH. KUNER, *Data Protection Law* cit., pp. 227 ss.

⁴³ THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 2.

⁴⁴ Così L.A. BYGRAVE, *Determining Applicable Law Pursuant to European Data Protection Legislation*, in *Computer Law and Security Report*, 2000, pp. 252 ss., a p. 255; CH. KUNER, *Internet Jurisdiction and Data Protection Law* cit., p. 176; J. GOLDSMITH, T. WU, *Who Controls the Internet? Illusions of a Borderless World*, Oxford, 2006, p. 175; F. RIGAUX, *Libre circulation des données* cit., p. 425.

⁴⁵ Cfr. THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., p. 8, 10 e 21; ID., *Working Document Privacy on the Internet - An integrated EU Approach*

Per restringere l'esorbitante ambito di estensione della lett. c, il «Gruppo Articolo 29» ha suggerito di introdurre un requisito soggettivo come presupposto di applicabilità di questa disposizione: sotto questo aspetto, l'utilizzo di «strumenti, automatizzati o non automatizzati» implicherebbe non soltanto un'effettiva attività di trattamento di dati personali da parte del responsabile, ma anche la «chiara intenzione» (*clear intention*) del responsabile di trattare dati personali⁴⁶, che non potrebbe riscontrarsi in assenza di una specifica volontà — o quantomeno di una ragionevole consapevolezza — di utilizzare, per il trattamento dei dati personali, strumenti situati nel territorio dello spazio economico europeo.

5. La natura giuridica dell'art. 4

L'intitolazione dell'art. 4 («Diritto nazionale applicabile») e il testo del considerando 18 («è opportuno assoggettare... [il trattamento dei dati personali] alla legge di tale Stato...») hanno indotto autorità di controllo e istituzioni a interpretare lo stesso art. 4 come «an explicit provision on the applicable law⁴⁷».

Persino il «Gruppo Articolo 29» ha ritenuto che «the directive itself fulfils the role of a so-called 'rule of conflict' and no recourse to other existing criteria of international private law is necessary», conclusione sulla quale ha concordato anche il Garante europeo della protezione dei dati personali⁴⁸. D'altra parte, la direttiva non dichiara esplicitamente di non voler introdurre norme supplementari di diritto internazionale privato: questa omissione in effetti potrebbe avallare *a contrario* il convincimento relativo alla funzione internazionalprivatistica svolta dell'art. 4, specialmente dopo la sentenza della Corte di giustizia nel caso *eDate Advertising*⁴⁹. In questa

to *On-line Data Protection*, doc. WP 37 del 21 novembre 2000, p. 28.

⁴⁶ THE ARTICLE 29 WORKING PARTY, *Working Document on Determining the International Application of EU Data Protection Law* cit., pp. 9 ss.; ID., *Opinion 8/2010 on Applicable Law* cit., p. 20.

⁴⁷ THE ARTICLE 29 WORKING PARTY, *Working Document on Determining the International Application of EU Data Protection Law* cit., p. 5. Cfr. anche la Prima relazione della Commissione sull'applicazione della direttiva cit., par. 4.4.1.

⁴⁸ Cfr., rispettivamente, THE ARTICLE 29 WORKING PARTY, *Working Document on Determining the International Application of EU Data Protection Law* cit., p. 6; THE EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion on the Communication from the Commission* cit., par. 122.

⁴⁹ Corte di giustizia, 25 ottobre 2011, *e Date Advertising GmbH c. X, Olivier Martinez e Robert*

pronuncia, la Corte ha affermato che l'art. 3 della direttiva 2000/31/CE, sul commercio elettronico⁵⁰, è una clausola «mercato interno» che, data la mancanza di armonizzazione a livello dell'Unione relativamente ai servizi informatici di tipo commerciale, per garantirne la libertà di circolazione nel mercato interno, assoggetta questi servizi alla legislazione nazionale dello Stato membro di stabilimento del prestatore, in conformità al principio dello Stato di origine. L'art. 3 della direttiva 2000/31/CE non svolge quindi una funzione internazionalprivatistica, «destinata a dirimere un conflitto specifico tra più diritti applicabili⁵¹», come può evincersi anche dall'art. 1, par. 4 della stessa direttiva, che dichiara di non voler introdurre «norme supplementari di diritto internazionale privato». Al contrario, la direttiva 95/46/CE non dichiara esplicitamente l'intenzione di non voler introdurre nuove norme di diritto internazionale privato: questo silenzio giustificerebbe quindi, alla luce della sentenza della Corte di giustizia nel caso *eDate Advertising*, la conclusione secondo la quale l'art. 4 della direttiva stessa costituisce «the first and only set of rules in an international data protection instrument to deal specifically with the determination of applicable law⁵²». In realtà, tuttavia, nemmeno l'art. 4 della direttiva 95/46/CE contiene norme di diritto internazionale privato. L'art. 4 si limita a determinare l'ambito territoriale di applicazione delle misure legislative nazionali degli Stati membri che recepiscono la direttiva: in linea con la finalità di armonizzazione completa perseguita dalla direttiva, questa

Martinez c. MGN Ltd, nelle cause riunite C-509/09 e C-161/10, non ancora pubbl., par. 60 ss.

⁵⁰ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (direttiva «e-commerce» o «commercio elettronico»), in *G.U.*, L 178 del 17 luglio 2000, pp. 1 ss.

⁵¹ Corte di giustizia, 25 ottobre 2011, *eDate Advertising GmbH* cit., par. 61. Anzi, secondo la Corte, dall'art. 1, n. 4, della direttiva, letto alla luce del considerando 3, emerge che, in linea di principio, gli Stati membri ospitanti sono liberi di designare, in base al proprio rispettivo sistema di diritto internazionale privato, le norme sostanziali applicabili, purché non ne derivi una restrizione della libera prestazione dei servizi del commercio elettronico (par. 62. Cfr., sul punto, cfr. M. FALLON, J. MEEUSEN, *Le commerce électronique, la directive 2000/31/CE et le droit international privé*, in *Rev. critique*, 2002, pp. 435 ss.). Infatti, la legge applicabile alle obbligazioni extracontrattuali che nascono da una violazione del diritto alla protezione dei dati personali ricade al di fuori del regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio dell'11 luglio 2007 sulla legge applicabile alle obbligazioni extracontrattuali («Roma II»), in *G.U.*, L 199 del 31 luglio 2007, pp. 40 ss., che esclude dal campo di applicazione del regolamento «le obbligazioni extracontrattuali che derivano da violazioni della vita privata e dei diritti della personalità, compresa la diffamazione» (art. 1, par. 2, lett. g).

⁵² L.A. BYGRAVE, *Determining Applicable Law* cit., p. 252.

norma uniforme pienamente «la portata territoriale di applicazione delle normative degli Stati membri in materia di protezione dei dati»⁵³. L'art. 4 è quindi una regola di applicabilità della direttiva⁵⁴, poiché fissa unilateralmente l'ambito territoriale di applicazione delle regole materiali alle quali accede, a prescindere dai criteri di applicabilità nello spazio eventualmente dettati dal diritto internazionale privato in vigore nel singolo Stato membro. Tuttavia, visto il rilievo attribuito dalla Commissione all'art. 4 nel quadro del perseguimento delle finalità dell'atto⁵⁵, a questa norma resta applicabile la giurisprudenza della Corte di giustizia secondo la quale il giudice nazionale deve garantire l'applicazione delle disposizioni impe-

⁵³ Cfr. par. 58 delle conclusioni dell'avv. gen. N. Jääskinen nel caso *Google Spain SL* cit., e considerando 8 della direttiva. In questo senso anche la comunicazione della Commissione *Un approccio globale* cit., par. 2.2.1., e le sentenze della Corte di giustizia, 24 novembre 2011, *ASNEF e FECEMD* cit., par. 29; 20 maggio 2003, *Rechnungshof e Österreichischer Rundfunk* cit., par. 100; 6 novembre 2003, *Bodil Lindqvist* cit., par. 96-97. Più in generale, cfr. sul punto M. MIGLIAZZA, *Profili internazionali ed europei del diritto all'informazione e alla riservatezza*, Milano, 2004, pp. 5 ss.

⁵⁴ Questa nozione è stata teorizzata da M. FALLON, *Les règles d'applicabilité en droit international privé*, in TH. AFSCHRIFT et al. (éds.), *Mélanges offerts à Raymond Vander Elst*, vol. I, Bruxelles, 1986, pp. 285 ss.; ID., *Les conflits de lois et de juridictions dans un espace économique intégré. L'expérience de la Communauté européenne*, in *Recueil des cours*, 1995-III, t. 253, pp. 9 ss., spec. pp. 180 ss.; ID., *Approche systémique de l'applicabilité dans l'espace de Bruxelles I et de Rome I*, in J. MEEUSEN, M. PERTEGÁS SENDER, G. STRAETMANS (eds.), *Enforcement of International Contracts in the European Union: Convergence and Divergence between Brussels I and Rome I*, Antwerp-Oxford-New York, 2004, p. 127 ss., a pp. 131; S. FRANCO, *L'applicabilité du droit communautaire dérivé au regard des méthodes du droit international privé*, Bruxelles, 2005, pp. 27 ss. Specificamente, sull'art. 4 della direttiva, cfr. M. FALLON, S. FRANCO, *Towards Internationally Mandatory Directives for Consumer Contracts?*, in J. BASEDOW, I. MEIER, A.K. SCHNYDER, T. EINHORN, D. GIRSBERGER (eds.), *Private Law in the International Arena. Liber Amicorum Kurt Siehr*, 2000, The Hague, pp. 155 ss., a p. 165. Per un confronto tra *règle directe d'applicabilité* e criteri di collegamento internazionalprivatistici, cfr. F. RIGAUX, M. FALLON, *Droit international privé*, 3ème éd., Bruxelles, 2005, pp. 125 ss., spec. A p. 129: «Il y a identité dans la fonction mais différence dans la méthode. Quant à la fonction, l'une et l'autre tendent à résoudre un conflit de lois, en déterminant la règle matérielle applicable à une situation internationale qui, par sa nature, peut être régie par le droit d'États différents. Quant à la méthode, la règle de rattachement prend pour hypothèse la situation particulière — ou rapport de droit — alors que la règle directe d'applicabilité prend pour hypothèse les règles matérielles dont l'applicabilité est visée. Cette différence a un effet sur l'objet de chacune de ces règles (...): alors que l'objet de la règle de rattachement s'étend à un ordre juridique considéré dans son ensemble, l'objet de la règle d'applicabilité se réduit à un jeu déterminé de règles matérielles. De plus, dans la seconde, il y a identité entre l'hypothèse de la règle et son objet, l'un et l'autre étant constitués des règles matérielles même dont l'applicabilité est en question».

⁵⁵ V. *supra*, nota 3.

relative di una direttiva, necessarie per la realizzazione degli obiettivi del mercato interno, malgrado l'applicazione di una legge regolatrice diversa. Il giudice nazionale, inoltre, in considerazione del carattere di armonizzazione piena che è proprio della direttiva, dovrà attenersi al principio di interpretazione conforme adeguando l'applicazione delle norme nazionali di diritto internazionale privato, ove possibile, alle richieste della direttiva comunitaria. Pertanto, è vero che l'art. 4 della direttiva non ha armonizzato il diritto internazionale privato degli Stati membri relativamente alla legge applicabile al trattamento dei dati personali; è da escludere, tuttavia, che possano interferire con questa norma eventuali previsioni divergenti o confliggenti del diritto internazionale privato degli Stati membri, che incrinerebbero l'uniformità nella determinazione dell'ambito territoriale di applicazione della disciplina comunitaria relativa alla protezione dei dati personali⁵⁶, e quindi il suo effetto utile.

6. I vizi argomentativi dell'Avvocato generale e della sentenza della Corte di Giustizia

Il rinvio pregiudiziale alla Corte di giustizia nel caso *Google Spain e Google Inc.* comprende, in particolare, quattro quesiti relativi specificamente all'ambito territoriale di applicazione della legislazione nazionale spagnola in materia di protezione dei dati. Il primo quesito verte sulla nozione di «stabilimento» prevista dall'art. 4, par. 1, lett. a) della direttiva; il secondo e il terzo riguardano i casi in cui si può considerare che venga fatto ricorso a «strumenti automatizzati o non automatizzati», situati nel territorio di uno Stato membro, ai sensi dell'art. 4, par. 1, lett. c); mentre l'ultimo, proposto per il caso nel quale la Corte dovesse ritenere inapplicabile l'art. 4 della direttiva, chiede se, alla luce dell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, che sancisce il diritto fondamentale al trattamento dei dati a carattere personale, debba essere eventualmente applicata la legislazione nazionale di attuazione dello Stato membro in cui si situa «il centro di gravità del conflitto», nel quale sarebbe asseritamente «possibile ottenere una tutela più efficace dei diritti dei cittadini dell'Unione». In via preliminare, la Corte chiarisce innanzitutto che Google Inc. è un «responsabile del trattamento» di dati personali ex art. 2, lett. b) e d) della direttiva. Per arrivare a questa conclusione, la Corte estende ai motori di ricerca la sua giurisprudenza precedente sui siti internet generalisti,

⁵⁶ Cfr. le conclusioni dell'avv. gen. N. JÄÄSKINEN nel caso *Google Spain SL* cit., par. 58.

dichiarando che la visualizzazione di dati personali su una pagina dei risultati di Google costituisce un autonomo «trattamento di dati personali», ex art. 2, lett. b) della direttiva, che «si distingue da e si aggiunge a quello effettuato dagli editori di siti web, consistente nel far apparire tali dati su una pagina internet⁵⁷». Responsabile del trattamento dei dati personali è, secondo la Corte, il gestore del motore di ricerca, in qualità di soggetto che, ai sensi dell'art. 2, lett. d della direttiva, determina, «insieme ad altri [cioè, insieme agli editori dei siti internet indicizzati], le finalità e gli strumenti del trattamento di dati personali⁵⁸». Chiarita la sussistenza di queste condizioni preliminari, la Corte inizia a verificare se, date le circostanze del caso di specie, la lett. a) dell'art. 4, par. 1 — dettata, come si è visto, per i responsabili del trattamento stabiliti nel territorio di uno Stato membro — sia applicabile anche a Google Inc., che ha la propria sede negli Stati Uniti. Tenuto conto delle incertezze e delle difficoltà applicative che, come si è visto, sono sollevate dalla lett. c) dell'art. 4, par. 1, prevista per i responsabili del trattamento non stabiliti, non c'è da stupirsi se i giudici insistono su qualsiasi mezzo interpretativo suscettibile di estendere l'applicazione della lett. a) a Google Inc. Da questo punto di vista, non è difficile per la Corte accertare che Google Spain costituisce uno «stabilimento» di Google Inc. nel territorio di uno Stato membro, ai sensi della lett. a) dell'art. 4, par. 1. Google Spain difatti si dedica «all'esercizio

⁵⁷ Cfr. sentenza cit., par. 35. Nel senso più ampio secondo il quale l'operazione consistente nel far comparire su una pagina web il nome e il cognome di una persona debba esser considerata un «trattamento di dati personali» ex art. 2, lett. b) della direttiva, v. già Corte di giustizia, 6 novembre 2003, *Bodil Lindqvist* cit., par. 25. Cfr. L. BURGORGUE-LARSEN, *Publication de données à caractère personnel sur internet, liberté d'expression et protection de la vie privée*, in *Rec. Dalloz*, 2004, *Jur.*, pp. 1062 ss. Sull'ampiezza della nozione di «dati personali» così come definiti dall'art. 2, lett. a della direttiva, cfr. Corte di giustizia, 20 maggio 2003, *Rechnungshof e Österreichischer Rundfunk* cit., par. 43; 7 maggio 2009, *Rijkeboer* cit., par. 59. Sulla protezione della *privacy* in riferimento all'attività dei motori di ricerca, v. B. VAN DER SLOOT, F. ZUIDERVEEN BORGESIU, *Google and Personal Data Protection*, in A. LÓPEZ-TARRUELLA (ed.), *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, Heidelberg, 2012, pp. 75 ss.

⁵⁸ Cfr. sentenza cit., par. 40. Invece, l'avv. gen. N. JÄÄSKINEN, richiamandosi alle osservazioni contenute in THE ARTICLE 29 WORKING PARTY, *Opinion 4/2007 on the concept of personal data*, doc. WP 136 del 20 giugno 2007, p. 17; Id., *Opinion 1/2008 on data protection issues related to search engines* cit., p. 8, 14, aveva escluso, sulla base del principio di proporzionalità, che un motore di ricerca possa esser considerato, in linea di principio, «responsabile del trattamento» effettuato su pagine *web source* di terzi, considerato che generalmente il motore di ricerca non esercita alcun controllo sui dati personali contenuti in tali pagine (conclusioni cit., par. 83), ad eccezione del caso nel quale il motore di ricerca non si limiti alle funzioni esclusivamente passive di semplice intermediario, ma eserciti un effettivo controllo sui dati (conclusioni cit., par. 91 e 93).

effettivo e reale dell'attività [economica] mediante un'organizzazione stabile», in conformità al considerando 19 della direttiva, poiché agisce in qualità di agente e rappresentante commerciale di Google Inc. per le sue attività pubblicitarie e promozionali sul mercato spagnolo. Google Spain è una filiale di Google Inc., cioè una controllata con autonoma personalità giuridica. Pertanto, ai fini dell'art. 4, par. 1, lett. a), Google Inc. deve ritenersi «stabilita» in Spagna tramite Google Spain⁵⁹, a prescindere dalla differenze attività economica da essa svolta. Alla stessa conclusione era giunto anche l'avv. gen. Jääskinen, che aveva affermato che le controllate stabilite da Google Inc. in vari Stati membri dell'Unione «chiaramente costituiscono stabilimenti ai sensi dell'articolo 4, par. 1, lett. a della direttiva⁶⁰». Questo sillogismo è tuttavia viziato da una forzatura interpretativa, evidente nelle conclusioni dell'avv. gen. Jääskinen. Infatti, per avallare la tesi secondo la quale Google Inc. sarebbe un «responsabile del trattamento» stabilito, l'avvocato generale è costretto ad affermare che la determinazione della legislazione nazionale di trasposizione applicabile rappresenterebbe una «questione preliminare», alla quale non dovrebbe applicarsi la definizione di «responsabile del trattamento» contenuta nella direttiva, poiché un operatore economico, costituito da una capogruppo e dalla filiale estera, dovrebbe esser considerato «come una entità singola», nel quadro dell'appartenenza allo stesso gruppo: pertanto, ai fini dell'analisi relativa alla sussistenza dei requisiti di applicabilità territoriale della direttiva, non dovrebbe «guardarsi alle sue singole attività relative al trattamento di dati personali o ai differenti gruppi di interessati ai quali queste si riferiscono⁶¹». Questa argomentazione riecheggia la dottrina dell'«unità economica» (*single economic entity*), utilizzata dalla Corte di giustizia per imputare alla *holding* la responsabilità per il comportamento anticoncorrenziale della controllata *ex art.* 101 TFUE⁶². Questo apre indubbiamente scenari stimolanti, sotto il profilo della considerazione del trattamento dei dati personali dal punto di vista della concorrenza e del mercato; tuttavia, al momento, le conclusioni dell'avvocato generale non sono sorrette da alcun dato testuale. In realtà, è evidente che le definizioni contenute nella direttiva si applicano anche all'art. 4 della direttiva stessa, nel quale sono contenuti i criteri di applicabilità territoriale delle misure

⁵⁹ Sentenza cit., par. 49.

⁶⁰ Conclusioni cit., par. 64.

⁶¹ Conclusioni cit., par. 66.

⁶² Cfr., nella giurisprudenza più recente, Corte di giustizia, 24 ottobre 1996, *Viho Europe BV*, in causa C-73/95P, in *Racc.*, 1996, pp. I-5457 ss., par. 16 (e giurisprudenza *ivi cit.*); 10 settembre 2009, *Akzo Nobel NV*, in causa C-97/08, in *Racc.*, 2009, p. I-8237, par. 61.

nazionali di recepimento, che non sono oggetto di una «questione preliminare», che ricadrebbe asseritamente al di fuori delle previsioni della direttiva, ma sono disciplinate da precise disposizioni dettate dalla stessa. In secondo luogo, è facile constatare che tanto l'art. 4, par. 1, quanto il considerando 19 della direttiva non si riferiscono ad «un'impresa» stabilita, ciò che potrebbe autorizzare la considerazione unitaria della società madre e della filiale appartenenti al medesimo gruppo societario, ma si riferiscono ad un «responsabile del trattamento» stabilito nel territorio di uno Stato membro. In altre parole, l'art. 4, par. 1 lett. a) è applicabile soltanto al trattamento di dati personali effettuato nel contesto delle attività *non di un'imprenditore stabilito*, ma di un «responsabile del trattamento» stabilito nel territorio di uno Stato membro. Google Inc. potrà essere stabilita nell'Unione europea in qualità di impresa tramite la sua filiale, ma non lo è in qualità di «responsabile del trattamento» di dati personali. Infatti, in conformità all'art. 2, lett. d) della direttiva, Google Inc. e Google Spain rappresentano due differenti «responsabili del trattamento», perché ciascuna delle due determina indipendentemente dall'altra «le finalità e gli strumenti» del trattamento di due categorie diverse di dati personali: Google Inc. è esclusivamente responsabile del trattamento dei dati personali visualizzati dagli utenti del motore di ricerca; Google Spain è responsabile soltanto del trattamento ai dati personali dei suoi clienti, acquirenti di inserzioni pubblicitarie. Anche se la visualizzazione dei risultati di una ricerca effettuata su Google con il nome di una persona può accompagnarsi alla contemporanea visualizzazione di annunci pubblicitari o di *link* sponsorizzati, il trattamento dei dati personali effettuato da Google Inc. in riferimento alle attività del motore di ricerca è totalmente indipendente dal trattamento dei dati personali relativi agli inserzionisti pubblicitari, effettuato da Google Spain, che non interferisce nel trattamento effettuato dalla capogruppo Google Inc. Di conseguenza, l'art. 4, par. 1, lett. a), interpretato alla luce del considerando 19 e dell'art. 2, lett. d) della direttiva, induce a ritenere non che Google Inc. sia un «responsabile del trattamento» stabilito nel territorio di uno Stato membro attraverso la filiale Google Spain, bensì che Google Inc. e Google Spain siano due diversi «responsabili del trattamento», uno stabilito e l'altro non stabilito nel territorio dell'Unione europea. L'interpretazione dell'avvocato generale sarebbe corretta soltanto se il responsabile del trattamento dei dati visualizzati dal motore di ricerca coincidesse con il responsabile del trattamento dei dati relativi alle inserzioni pubblicitarie, ipotesi che tuttavia dev'essere esclusa nel caso di specie, come risulta dai fatti di causa esposti dal giudice del

rinvio. Una volta ritenuto che Google Inc. è stabilita in Spagna attraverso la sua filiale Google Spain, alla Corte resta tuttavia ancora da verificare la sussistenza del requisito cruciale per l'applicazione della lett. *a*, e cioè la condizione che il trattamento dei dati personali sia effettuato nel «contesto delle attività dello stabilimento» del responsabile del trattamento nello Stato membro nel quale è stabilito. In questa prospettiva, Google Inc. potrebbe essere assoggettato alla misura spagnola di trasposizione della direttiva soltanto a condizione che il trattamento di dati personali visualizzati dal motore di ricerca ricada «nel contesto dell'attività» commerciale esercitata dalla filiale nel territorio di uno Stato membro.

In questa prospettiva, l'avv. gen. Jääskinen aveva proposto alla Corte di dichiarare che quando il gestore di un motore di ricerca, che effettua un trattamento di dati personali, apre in uno Stato membro una filiale *che orienti le proprie attività verso clienti del suddetto Stato membro*, deve ritenersi che effettui un trattamento dei dati personali «nel contesto delle attività» della controllata europea, a prescindere dal luogo nel quale sono tecnicamente trattati i dati, anche se la controllata si limita a promuovere e a vendere spazi pubblicitari sulla pagina dello stesso motore di ricerca⁶³. Infatti, osservava l'avvocato generale, la ragione per l'offerta gratuita di servizi da parte dei motori di ricerca è costituita dalla presenza di pubblicità mediante parole chiave sulla pagina dei risultati: «i fornitori commerciali di servizi di motore di ricerca su Internet offrono i propri servizi di localizzazione delle informazioni nell'ambito di un'attività economica volta a ricavare proventi dalla pubblicità tramite parole chiave⁶⁴». È quindi il servizio di vendita di spazi e inserzioni pubblicitarie *indirizzato al pubblico di un determinato Stato membro* a garantire la redditività del servizio gratuito di motore di ricerca. Lo stabilimento di filiali incaricate di occuparsi della pubblicità in sede locale (filiali che la Corte aveva definito nella sua giurisprudenza precedente prestatori di «un servizio di posizionamento a pagamento» degli operatori economici sul mercato pubblicitario⁶⁵) consente infatti a Google di orientare i propri servizi con modalità differenti verso Stati differenti, in funzione della «diversificazione nazionale» dell'attività del motore di ricerca, personalizzando la visualizzazione dei *link* sponsorizzati e delle inserzioni pubblicitarie a seconda della localizzazione geografica dell'utente del servizio. In questa prospettiva, l'avvocato generale ritiene che il trat-

⁶³ Conclusioni cit., par. 65 e 68.

⁶⁴ Conclusioni cit., par. 64, 124.

⁶⁵ Corte di giustizia, 23 marzo 2010, *Google France SARL e Google Inc. c. Louis Vuitton Malletier SA et al.*, nelle cause riunite da C-236/08 a C-238/08, in *Racc.*, 2010, pp. I-2417 ss., par. 23 ss.

tamento di dati personali relativo al motore di ricerca sia effettuato «nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio di uno Stato membro» se tale stabilimento, *orientando verso i cittadini e i residenti di quello Stato le proprie attività* di vendita di pubblicità nella pagina del motore di ricerca, «funge da collegamento per il servizio di posizionamento [del motore di ricerca] per il mercato pubblicitario di tale Stato membro», anche se le operazioni tecniche di trattamento dei dati sono svolte altri Stati membri, o anche in Stati terzi⁶⁶.

Questo aspetto delle conclusioni, nella parte in cui si sostiene che la società controllante, responsabile del trattamento di dati personali, dovrebbe essere trattata unitariamente con la propria filiale locale, nel quadro della direttiva, se il servizio gratuito di motore di ricerca è finanziato dal reddito generato da tale filiale, richiama inevitabilmente la giurisprudenza della Corte di giustizia relativa al finanziamento per compensazione tramite sovvenzioni incrociate delle attività economiche oggetto di obblighi di servizio di interesse economico generale *ex art.* 106, par. 2 TFUE⁶⁷. Ancora una volta, tuttavia, questa argomentazione presagisce significativi sviluppi futuri, specie sotto l'aspetto della qualificazione del gestore di un motore di ricerca come incaricato di un servizio di interesse economico generale, o di un servizio universale, ma non è di per sé sufficiente a soddisfare il requisito del «contesto delle attività». Evidentemente, il fatto che i servizi pubblicitari commercializzati da Google Spain siano a pagamento crea sì le condizioni finanziarie per la redditività dell'attività gratuita di Google Inc., *ma non le condizioni tecniche* per l'offerta del servizio relativo al motore di ricerca: ed è soltanto il fatto di aver predisposto tutte le condizioni tecniche necessarie per offrire un servizio di motore di ricerca, *non il fatto di percepire un compenso per tale servizio*, a determinare il «contesto delle attività» rispetto alle quali è funzionale il trattamento dei dati personali⁶⁸. E il richiamo al fatto che, attraverso le proprie filiali nazionali, Google Inc. *orienta le proprie attività verso i cittadini e i residenti di determinati Stati membri* è totalmente estraneo ai criteri posti dalla direttiva. In realtà, come

⁶⁶ Conclusioni cit., par. 67 ss.

⁶⁷ Cfr. la definizione di «servizio universale» all'art. 3. Disponibilità del servizio universale, della direttiva 2002/22/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva «servizio universale»), in *G.U.*, L 108 del 24 aprile 2002, p. 51 ss. Sulla giurisprudenza della Corte di giustizia in tema di sovvenzioni incrociate, cfr. W. SAUTER, *Services of General Economic Interest and Universal Service in EU Law*, in *Eur. Law Rev.*, 2008, pp. 167 ss.

⁶⁸ V., per analogia, l'affermazione contenuta nella sentenza della Corte di giustizia, 23 marzo 2010, *Google France SARL* cit., par. 57.

si vedrà, questo aspetto si riferisce, senza nominarla, alla proposta della Commissione relativa al nuovo regolamento di disciplina del trattamento dei dati personali, che modifica in questo senso i criteri di applicabilità territoriale della direttiva per i responsabili del trattamento non stabiliti. La Corte, malgrado l'intrinseca debolezza dell'argomentazione, accoglie le conclusioni dell'avvocato generale, e dichiara a sua volta che il trattamento di dati personali realizzato da un motore di ricerca avente uno stabilimento in uno Stato membro è effettuato «nel contesto delle attività dello stabilimento del responsabile del trattamento» in tale Stato membro, qualora esso sia destinato a garantire la promozione e la vendita di spazi pubblicitari che servono a rendere economicamente redditizio il servizio offerto dal motore di ricerca, e tale motore «è altresì lo strumento che consente lo svolgimento di dette attività». In questo caso, infatti, le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato risulterebbero «inscindibilmente connesse»⁶⁹. Di conseguenza, la Corte conclude che il trattamento di dati personali è effettuato dal motore di ricerca «nel contesto dell'attività pubblicitaria e commerciale dello stabilimento del responsabile del trattamento nel territorio di uno Stato membro»⁷⁰ qualora il gestore di un motore di ricerca apra in uno Stato membro una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca, l'attività della quale *si dirige agli abitanti di detto Stato membro*⁷¹.

La conclusione della Corte inverte totalmente i termini della questione: se il servizio relativo al motore di ricerca è, come afferma la stessa Corte, «lo strumento che consente lo svolgimento [delle] attività» di promozione e vendita di spazi pubblicitari e di *link* sponsorizzati sulla pagina del motore di ricerca, è giocoforza ammettere che senza il motore di ricerca non esisterebbe alcuna raccolta pubblicitaria. Quindi, è l'attività commerciale di vendita di pubblicità che è effettuata «nel contesto delle attività» del motore di ricerca (che comprendono il trattamento dei dati personali oggetto della sentenza), e non il contrario, come afferma invece la Corte. In realtà, l'art. 4, par. 1 della direttiva non si limita a richiedere che le attività del responsabile del trattamento e quelle dello stabilimento della sua filiale nel territorio di uno Stato membro siano «connesse» — sia pure «inscindibilmente connesse» —, ma esige che il trattamento di dati personali venga effettuato «nel contesto delle attività dello stabilimento del responsabile del trattamento». Questa condizione presuppone non una generica «con-

⁶⁹ Sentenza cit., par. 56.

⁷⁰ Sentenza cit., par. 57.

⁷¹ Sentenza cit., par. 60.

nessione », come vuole la Corte, ma una precisa relazione di strumentalità tra il trattamento dei dati personali e l'attività economica dello stabilimento situato nel territorio di uno Stato membro: il trattamento di dati personali dev'essere funzionale alla specifica attività economica svolta nello stabilimento del responsabile del trattamento che è situato nel territorio dello Stato membro. Il requisito del «contesto delle attività» è soddisfatto soltanto quando il trattamento di quei determinati dati personali è richiesto da quella determinata attività economica svolta nello stabilimento del responsabile del trattamento situato nello Stato membro. Nella fattispecie, tuttavia, lo «stabilimento del responsabile del trattamento nello Stato membro», cioè Google Spain, svolge attività che non sono in relazione al trattamento di dati personali effettuato da Google Inc. Questo caso è proprio uno di quelli che, come si ricorderà, non ricade né nella lett. a) dell'art. 4, par. 1, visto che il trattamento di dati personali non è effettuato «nel contesto delle attività» esercitate dallo stabilimento nel territorio dello Stato membro; né nella lett. c), prevista per i responsabili del trattamento non stabiliti, poiché la Corte parte dal presupposto che Google Inc. sia stabilito, attraverso la sua filiale, nel territorio di uno Stato membro. La Corte decide tuttavia che l'«inscindibile connessione» è sufficiente per soddisfare il requisito del «contesto delle attività». Questa interpretazione è giustificata soltanto dall'esigenza di estendere il più possibile il diritto fondamentale alla tutela dei dati personali, al quale la Corte di giustizia attribuisce un rilievo prioritario nel quadro delle finalità della direttiva⁷², in un caso come quello ad oggetto, nel quale è coinvolto un cittadino dell'Unione, domiciliato in uno Stato membro, a fronte di un responsabile del trattamento stabilito al di fuori dello spazio economico europeo. Tuttavia, la lettura della Corte non ha alcun fondamento testuale nell'art. 4 della direttiva — né, probabilmente, ha alcun riscontro fattuale: infatti, la Corte non specifica mai, né nell'esposizione dei fatti di causa, né nella motivazione della sentenza, se nella pagina dei risultati della ricerca effettuata dal Costeja González con il proprio nome su Google comparissero effettivamente risultati sponsorizzati, che si attivano soltanto a condizione che la parola chiave attraverso la quale è effettuata la ricerca sia stata acquistata da un inserzionista. L'aver riscontrato la sussistenza di tutti i criteri di applicabilità previsti dalla lett. a) risparmia però ai giudici la necessità di effettuare la verifica, ben più complessa, relativa all'eventuale sussistenza delle condizioni di applicazione della lett. c) dell'art. 4, par. 1, oggetto del secondo e del terzo quesito del giudice del rinvio. L'interpretazione estensi-

⁷² Sentenza cit., par. 53 ss.

va delle condizioni di applicazione della legislazione nazionale di trasposizione della direttiva è peraltro in linea con il rilievo prioritario che la Corte attribuisce, nella sua giurisprudenza più recente, al diritto fondamentale alla tutela dei dati personali nel quadro delle finalità della direttiva, «come confermato segnatamente dall'art. 1, par. 1, e dai considerando 2 e 10 della direttiva medesima⁷³». Ancora una volta, tuttavia, la Corte omette qualsiasi riferimento al par. 2 dello stesso art. 1 della direttiva, che vieta agli Stati membri di restringere o ostacolare la libertà di circolazione dei dati personali nel mercato interno per motivi connessi alla tutela del diritto delle persone fisiche alla protezione dei dati personali. Con l'ultimo quesito pregiudiziale, l'*Audiencia nacional* chiedeva se, alla luce dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea, che sancisce il diritto fondamentale al trattamento dei dati a carattere personale, possa essere applicata nella fattispecie la misura nazionale di attuazione dello Stato membro in cui si situa «il centro di gravità del conflitto». Questo criterio, che è estraneo all'art. 4 della direttiva, si rinviene nelle conclusioni dell'avv. gen. Cruz Villalón nel caso *eDate Advertising*⁷⁴, relativo alla competenza giurisdizionale per violazioni di diritti della personalità avvenute attraverso la pubblicazione di informazioni su internet. L'avvocato generale aveva proposto un «criterio aggiuntivo di collegamento» rispetto a quelli consentiti dalla giurisprudenza della Corte di giustizia sull'art. 5, n. 3 del regolamento «Bruxelles I⁷⁵». Questa norma, che, «in materia di illeciti civili dolosi o colposi», consente di convenire una persona domiciliata in uno Stato membro «davanti al giudice del luogo in cui l'evento dannoso è avvenuto o può avvenire», è stata interpretata, a partire dalla sentenza *Shevill* della Corte di giustizia, nel senso per cui, in materia di diffamazione a mezzo stampa, la competenza spetta al giudice del luogo nel quale è stato posto in essere il comportamento del danneggiante, oppure al giudice del luogo, eventualmente diverso, nel quale la vittima ha subito il danno⁷⁶. Ciò posto,

⁷³ V. sentenza cit., par. 58 (v. anche la giurisprudenza cit. *supra*, nota 10).

⁷⁴ Conclusioni dell'avvocato generale P. CRUZ VILLALÓN presentate il 29 marzo 2011 nel caso *eDate Advertising* cit., par. 32 e 55 ss.

⁷⁵ Regolamento (CE) n. 44/2001 del Consiglio del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, in *G.U.*, L 12 del 16 gennaio 2001, pp. 1 ss. («Bruxelles I»), destinato a essere sostituito, con effetto dal 10 gennaio 2015, dal regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio del 12 dicembre 2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale, in *G.U.*, L 351 del 20 dicembre 2012, pp. 1 ss. («Bruxelles I bis »).

⁷⁶ Corte di giustizia, 7 marzo 1995, *Shevill*, in causa C-68/93, in *Racc.* 1995, pp. I-415 ss., par. 33. Su questa giurisprudenza cfr., per tutti, G. HOGAN, *The Brussels Convention*,

secondo l'avv. gen. Cruz Villalón, il «centro di gravità del conflitto» si troverebbe nel Paese nel quale il titolare del diritto della personalità possiede il proprio «centro di interessi», nel quale è più intenso il rischio di una violazione di un suo diritto, e nel quale esso subisce la lesione più grave e più facilmente prevedibile. Di conseguenza, questo luogo sarebbe quello nel quale il giudice si trova nella migliore situazione per valutare il conflitto tra i beni e gli interessi in gioco. L'avv. gen. Jääskinen tuttavia esclude, nelle sue conclusioni, qualsiasi rilievo del «centro di gravità del conflitto», osservando che la Carta dei diritti fondamentali dell'Unione europea non consente di estendere l'ambito di applicazione del diritto dell'Unione al di là delle competenze ad essa attribuite, né di introdurre competenze nuove per l'Unione o modificare quelle previste nei trattati⁷⁷. Infatti, se nel caso *eDate Advertising* si trattava soltanto di modificare eventualmente la lettura giurisprudenziale del testo del regolamento «Bruxelles I», nel caso *Google Spain* si tratterebbe di introdurre in via interpretativa un «nuovo elemento che faccia scattare l'applicazione territoriale della normativa nazionale di attuazione della direttiva⁷⁸» in assenza di riscontri testuali nell'art. 4 della direttiva. La Corte, che nel caso *eDate Advertising* non aveva accolto la proposta dell'avvocato generale, nel caso *Google Spain* ritiene di non doversi pronunciare, avendo già dato soluzione positiva al primo quesito proposto dal giudice del rinvio.

7. L'art. 3 della proposta di regolamento di riforma della direttiva. In particolare: il «Targeting Test»

Tanto le conclusioni dell'avv. gen. Jääskinen, quanto la decisione della Corte di giustizia sull'applicabilità territoriale della legislazione nazionale di trasposizione della direttiva non si spiegherebbero senza il riferimento

Forum Non Conveniens and the Connecting Factors Problem, in *Eur. Law Rev.*, 1995, pp. 471 ss.; A. GARDELLA, *Diffamazione a mezzo stampa e Convenzione di Bruxelles del 27 settembre 1968*, in *Riv. dir. int. priv. proc.*, 1997, p. 657 ss.; K. SIEHR, *European private international law of Torts. Violations of privacy and rights relating to the personality*, *ibid.*, 2004, pp. 1201 ss.

⁷⁷ Cfr. art. 51, *Ambito di applicazione*, par. 2 della Carta, sul quale cfr. Corte di giustizia, 5 ottobre 2010, *McB.*, in causa C-400/10 PPU, in *Racc.*, 2010, pp. I-8965 ss., par. 51 e 59; 15 novembre 2011, *Dereci*, in causa C 256/11, *ibid.*, 2011, p. I-11315, par. 71 ss.; 8 novembre 2012, *Iida*, in causa C 40/11, non ancora pubbl., par. 78; 26 febbraio 2013, *Åkerberg Fransson*, in causa C-617/10, non ancora pubbl., par. 23.

⁷⁸ Conclusioni cit., par. 54.

implicito alla proposta della Commissione relativa al regolamento di riforma della disciplina europea del trattamento dei dati personali, destinato a sostituire la direttiva. Tanto i giudici della Corte, quanto l'avvocato generale si riferiscono più volte, infatti, ad un fattore totalmente estraneo all'art. 4 della direttiva, e cioè al fatto che il responsabile del trattamento «si diriga» a cittadini o residenti nel territorio di uno Stato membro. Questa indicazione è contenuta soltanto nell'art. 3 della proposta della Commissione, nella parte nella quale definisce il campo di applicazione territoriale del nuovo regolamento a responsabili del trattamento non stabiliti nello spazio economico europeo⁷⁹.

L'art. 3 della proposta di regolamento che, a differenza dell'art. 4 della direttiva, costituisce un'autentica norma uniforme di diritto internazionale privato, di carattere unilaterale⁸⁰, ripropone lo schema dualistico della direttiva, prevedendo differenti condizioni di applicabilità per i responsabili del trattamento stabiliti in uno Stato membro e per i responsabili non stabiliti. Se il criterio di collegamento per i responsabili del trattamento stabiliti non è stato sostanzialmente modificato (è anche ribadito il requisito che il trattamento venga effettuato « nell'ambito delle attività di uno stabilimento » del responsabile o di un incaricato del trattamento nell'Unione⁸¹), il par. 2 dell'art. 3, applicabile ai responsabili del trattamento

⁷⁹ Cfr. considerando 136-138 della proposta.

⁸⁰ Infatti, poiché il regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile, sostituisce qualsiasi disposizione differente dell'ordinamento nazionale degli Stati membri. Pertanto, l'affermazione iniziale dell'art. 3, secondo la quale «[i]l presente regolamento si applica... » stabilisce in realtà un criterio di collegamento dell'atto in quanto parte di tutto il complesso del diritto nazionale di uno Stato membro. È indiscutibile, quindi, che l'art. 3 costituisca una norma internazionalprivatistica uniforme.

⁸¹ L'art. 3, par. 1 stabilisce che il regolamento si applica innanzitutto al trattamento dei dati personali effettuato « nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione », e prevede ancora, al par. 3 dell'art. 3, la medesima eccezione all'applicazione al responsabile del trattamento non stabilito nell'Unione europea relativa al caso « diplomatico » di applicazione della direttiva (v. anche considerando 22). Il criterio di collegamento non è più riferito esclusivamente all'ubicazione dello stabilimento del responsabile del trattamento, come nella direttiva, ma anche, in alternativa, allo stabilimento dell'«incaricato del trattamento», definito all'art. 4, par. 6 della proposta di regolamento come «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento». Cfr. anche l'art. 26, Incaricato del trattamento, e la nozione di nuova introduzione all'art. 24, Corresponsabili del trattamento, che può adattarsi alle nuove figure di intermediari di servizi emerse nella prassi. Per effetto di questa modifica, non è più necessario identificare con precisione il responsabile del trattamento, che in determinate situazioni può essere difficoltoso. Infine, su indicazione del «Gruppo Articolo 29», che raccomandava di ancorare l'applicazione del nuovo regolamento al prin-

non stabiliti, è invece del tutto nuovo. Questa disposizione afferma che il regolamento si applica al trattamento di dati personali di soggetti residenti nell'Unione effettuato un responsabile non stabilito «quando le attività di trattamento riguardano: *a)* l'offerta di beni o la prestazione di servizi ai suddetti residenti nell'Unione, oppure *b)* il controllo del loro comportamento» (così anche i considerando 20 e 21). In tutti questi casi, il principio di origine che era oggetto della lett. *c)* dell'art. 4, par. 1 della direttiva è sostituito da un principio di destinazione o, più precisamente, dal principio di prossimità, considerato che al trattamento dei dati personali sarà applicabile la legge dello Stato membro nel quale sono residenti (o si trovano fisicamente) le persone alle quali sono dirette le offerte commerciali⁸², o nei confronti delle quali sono effettuate azioni di *data tracking*, *data profiling* o *data mining*. Quindi, se il trattamento dei dati personali è relativo a persone residenti nell'Unione, si applica il regolamento anche se il responsabile del trattamento è stabilito in uno Stato terzo, e anche se le operazioni di trattamento sono effettuate tecnicamente al di fuori dello spazio economico europeo, qualora il trattamento riguardi l'offerta di beni o la prestazione di servizi indirizzate a residenti in uno Stato membro dell'Unione, oppure si risolva nel controllare il comportamento *online* delle persone interessate. Proponendo questo nuovo testo, la Commissione accetta (parzialmente) il suggerimento del «Gruppo Articolo 29» relativo all'introduzione di un «*targeting test*» per i responsabili del trattamento di dati personali non stabiliti, in vista dello stretto legame esistente tra le richieste relative alla protezione dei dati personali dei cittadini o dei residenti di uno Stato membro e le esigenze di tutela del consumatore nel mercato interno⁸³. Da questo punto di vista, il par. 2 dell'art. 3 avrebbe

inizio dello «sportello unico» («one-stop shop»), identificandolo con il principio del paese di origine (cfr. THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., pp. 15 ss., 29; nonché la comunicazione della Commissione *Salvaguardare la privacy in un mondo interconnesso* cit., p. 9), l'art. 4, par. 13 della proposta introduce la definizione di «stabilimento principale» nell'Unione del responsabile e dell'incaricato del trattamento (art. 51, par. 2 e considerando 27 e 98 della proposta di regolamento), che tuttavia resta senza riscontro nella delimitazione del campo di applicazione territoriale della proposta di regolamento, poiché non è ripresa dall'art. 3.

⁸² Anche se l'art. 3 non individua chiaramente lo Stato membro la cui legge regolatrice è applicabile: cfr. *Vice-President of the European Commission, EU Justice Commissioner Viviane Reding's intervention in the Justice Council, Brussels - European Commission SPEECH/13/1027* del 6 dicembre 2013.

⁸³ THE ARTICLE 29 WORKING PARTY, *Opinion 8/2010 on Applicable Law* cit., pp. 15 ss., 29. In questo senso anche L.A. BYGRAVE, *Determining Applicable Law* cit., p. 257. Anche nel commercio elettronico, la protezione dei singoli relativamente al trattamento dei dati personali è disciplinata esclusivamente dalla direttiva 95/46/CE e dalla dir.

il vantaggio di allineare sostanzialmente i criteri di determinazione della legge applicabile al trattamento dei dati personali effettuato da prestatori di servizi non stabiliti al criterio dell'«attività diretta con qualsiasi mezzo» al consumatore, *ex art. 6, par. 1, lett. b)* del regolamento «Roma I⁸⁴», e all'art. 15, par. 1, lett. c), relativo alla competenza giurisdizionale in caso di contratti conclusi da un consumatore, contenuto nel regolamento «Bruxelles I», al quale il legislatore si è ispirato per il regolamento «Roma I⁸⁵». Tuttavia, la proposta della Commissione non coincide completamente né con il regolamento «Roma I», né con il regolamento «Bruxelles I», nemmeno dopo gli emendamenti apposti dal Parlamento europeo in prima lettura, che anzi hanno avuto l'effetto di allontanarla ulteriormente dal modello originario. Di conseguenza, la giurisprudenza della Corte di giustizia sulla lett. c dell'art. 15, par. 1 del regolamento Bruxelles I, in particolare le sentenze nei casi *Pammer* e *Wintersteiger*⁸⁶, non troverebbero piena applicazione al «*targeting test*» per i responsabili del trattamento non stabiliti, con la conseguenza che potrebbero verificarsi ancora dei vuoti nella tutela del consumatore residente nell'Unione europea, dal punto di vista del trattamento dei dati personali. Tuttavia, tra gli emendamenti già apposti dal Parlamento europeo al testo dell'art. 3, par. 2 c'è, in particolare, una precisazione non superflua, tenendo conto proprio della sentenza *Google Spain*, e cioè l'indicazione secondo la quale il «*targeting test*», nella

97/66/CE cit.: l'art. 1, par. 5 della direttiva «commercio elettronico» afferma che la dir. non si applica: «b) alle questioni relative ai servizi della società dell'informazione oggetto delle dir. 95/46/CE e 97/66/CE». Sull'intersezione tra il diritto alla protezione dei dati personali e il commercio elettronico cfr., specificamente, CH. KUNER, *Beyond Safe Harbor: European Data Protection Law and Electronic Commerce*, in *Int'l Lawyer*, 2001, pp. 79 ss.

⁸⁴ Regolamento (CE) n. 593/2008 del Parlamento europeo e del Consiglio del 17 giugno 2008 sulla legge applicabile alle obbligazioni contrattuali («Roma I»), in *G.U.*, L 177 del 4 luglio 2008, p. 6 ss.

⁸⁵ Cfr., sul punto, P. PIRODDI, *La tutela del contraente debole nel regolamento Roma I*, Padova, 2012, spec. pp. 156 ss.

⁸⁶ Corte di giustizia, 7 dicembre 2010, *Pammer e Hotel Alpenhof*, nelle cause riunite C-585/08 e C-144/09, in *Racc.*, 2010, pp. I-12527 ss., par. 93; 19 aprile 2012, *Wintersteiger*, in causa C-523/10, non ancora pubbl. Sulla sentenza *Pammer* cfr., per tutti, V. PIRONON, *Dits et non-dits sur la méthode de la focalisation dans le contentieux - contractuel et délictuel - du commerce électronique*, in *Clunet*, 2011, pp. 915 ss.; M. BOGDAN, *Website Accessibility as a Basis for Jurisdiction under Art. 15(1)(C) of the Brussels I Regulation: Case Note on the ECJ Judgment Pammer and Alpenhof*, in *Yearbook Priv. Int. Law*, 2010, pp. 565 ss. Sulla sentenza *Wintersteiger*, cfr. B. CLARK, *Off piste? ECJ Decides Austrian Supreme Court's «Adwords» Jurisdiction Question in Wintersteiger*, in *Journ. Intell. Property. Law Pract.*, 2012, pp. 701 ss.

parte relativa all'offerta di beni o alla prestazione di servizi agli interessati nell'Unione europea, è applicabile «indipendentemente dall'obbligatorietà di un pagamento dell'interessato⁸⁷»: pertanto, non avrebbe alcun rilievo, ai fini del «*targeting test*», il fatto che le attività dell'operatore economico siano offerte a titolo gratuito invece che dietro compenso, nel momento in cui si «dirigono» a interessati cittadini o residenti nell'Unione europea. Questo conferma che i requisiti richiesti per l'applicazione territoriale della disciplina europea di protezione dei dati personali sono soddisfatti se sono state create le *condizioni tecniche necessarie* per la risposta da parte dei soggetti destinatari di un'offerta di beni o di servizi, a prescindere dalle condizioni economiche dell'offerta stessa. L'art. 3, par. 2 della proposta di regolamento è in grado di ridurre fortemente l'esorbitante ambito di applicazione della legislazione nazionale degli Stati membri, tuttora consentito dall'art. 4, par. 1, lett. c della direttiva. Peraltro, il nuovo regolamento dovrebbe continuare ad applicarsi a prescindere dal fatto che i dati personali siano raccolti e trattati al di fuori dello spazio economico europeo⁸⁸, precauzione che continua ad essere necessaria per disincentivare

⁸⁷ Risoluzione legislativa del Parlamento europeo del 12 marzo 2014 cit. L'introduzione di questa modifica è presumibilmente legata alla definizione di « servizi della società dell'informazione » come « qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi », effettuata dall'art. 2, lett. a) della direttiva commercio elettronico, che rinvia all'art. 1, n. 2, della direttiva del Parlamento europeo e del Consiglio n. 98/34/CE del 22 giugno 1998, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (in *G.U.*, L 204 del 21 luglio 1998, pp. 37 ss.), quale modificata dalla direttiva del Parlamento europeo e del Consiglio n. 98/48/CE del 20 luglio 1998 (in *G.U.*, L 217 del 5 agosto 1998, pp. 18 ss.). Cfr. anche il testo emendato del considerando 20. Il Parlamento europeo ha inoltre esteso in prima lettura la portata dell'art. 3, par. 2 della proposta della Commissione ai casi di trattamento effettuato non soltanto da un responsabile, ma anche da un « incaricato del trattamento » non soltanto nei confronti delle persone residenti in uno Stato membro, ma più in generale nei confronti degli « interessati nell'Unione »; infine, ha ampliato la sua applicabilità non soltanto al controllo del « comportamento » degli interessati, ma di rettamente al « controllo degli interessati nell'Unione ». La tendenza ad estendere l'applicabilità del regolamento consegue, ancora una volta, al carattere fondamentale del diritto alla protezione dei dati personali.

⁸⁸ Inoltre, nel caso dell'art. 3, par. 2, un responsabile del trattamento non stabilito nell'UE avrà ancora l'obbligo di designare un rappresentante nell'UE, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento: v. art. 25 della proposta di regolamento. Perplessità sul carattere eccessivamente restrittivo dell'art. 3, par. 2 della proposta sono state espresse nel «Parere del Comitato economico e sociale europeo in merito alla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali

la delocalizzazione in Stati terzi degli stabilimenti preposti alle operazioni tecniche di trattamento dei dati, e il conseguente rischio di elusione della disciplina europea tramite *forum shopping*.

Abstract

In Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, the Court of Justice interpreted, for the first time since the entry into force of the data protection directive, the connecting factors that determine the applicability of the directive to processing of personal data for EU member States. On account of the fundamental scope of the right to personal data protection, the Court of justice decided on extensive interpretation, therefore declaring that the search engine activities provided by Google Inc., which is established in the United States, are covered by the data protection directive, because of the establishment of a subsidiary of Google Inc. in the territory of a EU member State. This conclusion, which seems to be based on defective reasoning, allows an exorbitant reach of Member States' laws under the directive, and may obstruct access to the internal market for leading IT services providers that are established outside the EU territory. This judgment will arguably accelerate final approval of the long-awaited modernization of the data protection directive, that the Commission proposed in 2012, with a view to reform particularly the connecting factors determining the applicable law to the processing of personal data for EU member States.

e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati, doc. COM(2012)11 def. 2012/0011 (COD)), doc. 2012/C 229/17, in *G.U.*, C 229 del 31 luglio 2012. pp. 90 ss., par. 4.5.

Giovanni Sartor - Mario Viola De Azevedo Cunha

Il caso Google e i rapporti regolatori USA/EU

SOMMARIO: 1. Introduzione: divergenze e convergenze politico-giuridiche tra Europa e Stati Uniti - 2. La trasmissione dei dati sui passeggeri (PNR) e gli accordi SWIFT - 3. Il caso Snowden - 4. La discussione sul Regolamento sulla protezione dei dati - 5. Google- Spain: un conflitto giuridico o politico? - 6. Conclusione.

1. Introduzione: divergenze e convergenze politico- giuridiche tra Europa e Stati Uniti

La regolazione della protezione dei dati negli Stati Uniti e nell'Unione Europea presenta divergenze non solo in aspetti particolari, ma anche sulle ispirazioni più astratte. Infatti, benché i valori etico-giuridici e gli interessi economico-politici in gioco siano gli stessi negli Stati Uniti e nell'Unione, tali valori e interessi si presentano con diversa intensità nelle due sponde dell'Atlantico, cosicché ne risultano distinti indirizzi politici e giuridici, che si oppongono nel dibattito globale sulla protezione dei dati. L'evoluzione delle norme sociali e dei valori giuridici ha fatto sì che in Europa l'idea della *privacy* si collegasse a quella della dignità¹. Il valore giuridico della dignità ha molteplici radici, religiose, umanistiche e filosofiche, attinenti alle dimensioni dell'autodeterminazione, del rispetto e dell'eguaglianza, ma la sua tutela giuridica si collega originariamente al tentativo 'democratico' di garantire a tutti i cittadini attributi riservati alle classi privilegiate, cioè l'attributo aristocratico dell'onore e quello romantico di una personalità che si sviluppa liberamente, secondo la propria dinamica interiore. La tutela di questi attributi comporta l'esigenza di proteggere l'individuo rispetto alla circolazione d'informazioni che lo riguardano, suscettibili di incidere sulla sua immagine sociale. Si tratta di un'elaborazione che le culture giuridiche tedesca e francese compivano già

¹ Su questi aspetti, si vedano N.WONG, *Privacy: Charting its Developments and Prospects*. In M.KLANG e A.MURRAY. *Human Rights in the Digital Age* (2005), London: Glasshouse Press. p. 158.

nell'ottocento, cosicché il celeberrimo contributo di Warren e Brandeis², spesso considerato all'origine dell'idea di *privacy* quale controllo sulla circolazione delle informazioni personali, può forse considerarsi, alla luce di una storia globale del pensiero giuridico, come un trapianto parzialmente fallito³. Il valore della dignità ispira in particolare la disciplina europea sulla protezione dei dati, e con riferimento a questo valore l'esigenza di controllare la raccolta e la circolazione dei dati personali è stata affermata non solo nella legislazione e nella giurisprudenza comunitaria e nazionale, ma anche al supremo livello dell'ordinamento dell'Unione, nell'articolo 8 della Carta dei diritti fondamentali, dedicato al diritto alla protezione dei dati personali. Negli Stati Uniti invece, l'idea di *privacy* è rimasta prevalentemente incentrata sulla tutela dello spazio vitale dell'individuo, circoscritto dalla sua persona e proprietà, rispetto alle intrusioni da parte dello Stato, tanto nella raccolta d'informazioni quanto nella limitazione della libertà di scelta. A questa idea si ispira anche la giurisprudenza della Corte suprema, in una serie di celebri sentenze, come *Griswold v. Connecticut* (1965) e *Roe v. Wade* (1973).

Le due idee di *privacy*, come controllo 'dignitario' sulla propria rappresentazione sociale e come libertà privata da intrusioni pubbliche, sono peraltro presenti in entrambe le culture giuridiche, e non vi è incompatibilità tra esse, come provano non solo numerosi contributi dottrinali tesi a integrare le due prospettive⁴, ma anche il fatto che sia il diritto europeo, sia quello statunitense, contemplano entrambi gli aspetti, nella legislazione come nella giurisprudenza. Tuttavia, i diversi aspetti della *privacy* hanno diverso rilievo nelle due culture, così come hanno diverso rilievo i valori e gli interessi suscettibili di opporsi alla *privacy*. Ne risaltano diverse possibilità che la *privacy* possa essere lecitamente compressa nei conflitti con altri valori e interessi⁵.

In particolare, l'assoluta preminenza della libertà di espressione (*freedom of speech*) negli Stati Uniti limita l'ambito della protezione della *privacy* rispetto alla pubblicazione d'informazioni personali mediante ogni tipo di mezzi di comunicazione, Internet inclusa. Nell'ordinamento statunitense ogni informazione può essere in linea di principio comunicata al pubbli-

² S. WARREN e L. BRANDEIS, *The right to privacy* (1890), *Harvard Law Review*, 4:193-220.

³ V.J. WHITMAN, *The two western cultures of privacy: Dignity versus liberty* (2003- 4), *Yale Law Journal*, 113:1152-221.

⁴ V. tra tutti, W.L. PROSSER, *Privacy* (1960), *California Law Review*, pp. 389-407 e recentemente D.J. SOLOVE, *A taxonomy of privacy* (2006), *University of Pennsylvania Law Review*, pp. 154:477.

⁵ N. WONG, *Privacy: Charting ecc.* (2005). *op. cit.* p. 158.

co, con i soli limiti della proprietà intellettuale e di immagini di nudità.

Persino foto di nudità, prese con il consenso dell'interessato, ma pubblicate su Internet senza il suo consenso, possono essere successivamente distribuite in rete contro la volontà dello stesso⁶.

Inoltre, ogni informazione o immagine concernente comportamenti in luoghi aperti al pubblico, può essere liberamente distribuita, anche quando si metta l'informazione o immagine a disposizione di un pubblico più ampio e diverso rispetto a quello presente nel contesto originario⁷. Un limite può essere dato dall'esistenza di un'«aspettativa di *privacy*»⁸, ma questa aspettativa opera solo nei casi in cui l'interessato possa prevedere che l'informazione che lo riguarda non sarà raccolta ed elaborata o distribuita, e ciò corrisponda alle prevalenti norme sociali: di conseguenza ogni prassi limitativa della *privacy* che sia socialmente diffusa tende ad essere legittima. In particolare, la preminenza della libertà di espressione preclude, nel diritto statunitense, ogni spazio per il diritto all'oblio su Internet: se un'informazione è stata legittimamente diffusa al pubblico, può continuare a essere distribuita, e può essere ripubblicata senza limiti. Quindi, mentre negli ordinamenti europei il diritto all'oblio rispetto a informazioni pregiudizievoli per l'interessato e non più attuali è variamente riconosciuto⁹, negli Stati Uniti non c'è praticamente alcun limite alla

⁶ Si veda J. WHITMAN, *The two western ecc. op. cit.*, p. 1200. Recentemente peraltro alcuni Stati USA hanno emanato leggi che proibiscono la pubblicazione di immagini sessualmente esplicite senza il consenso dell'interessato, nel tentativo di contrastare il diffuso fenomeno del revenge porn (pornografia di vendetta, avente lo scopo di umiliare o imbarazzare).

⁷ Come esempio estremo, ricordiamo il caso di Oliver Sipple, che sventò eroicamente un attentato alla vita del presidente Gerald Ford, ma così facendo si espose alla curiosità della stampa, che ne rivelò l'orientamento omosessuale, tenuto fino ad allora nascosto alla famiglia. Sipple successivamente si suicidò (J. WHITMAN *The two western ecc.* [2003-4], *op. cit.* p. 1196).

⁸ Il Parlamento Europeo, modificando il testo della Proposta di Regolamento Generale sulla Protezione dei dati, ha incluso il requisito che sia soddisfatta la «ragionevole aspettativa» di *privacy* dell'interessato nell'Art. 6 lettera (f), quale condizione aggiuntiva per l'elaborazione giustificata da legittimi interessi del titolare, (PARLAMENTO EUROPEO, Risoluzione legislativa del 12 marzo 2014).

⁹ Per una trattazione dei diversi aspetti del diritto all'oblio, in Italia e all'estero, si vedano i contributi in F. PIZZETTI a cura di, *Il caso del diritto all'oblio* (2013), Giappichelli. Sugli aspetti comparati, v. in particolare O. POLLICINO e M. BASSINI, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, *ibid.*, pp. 185-228; Sul diritto all'oblio v. anche, tra gli altri: G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. Inf.* 2010, pp. 393-403. G. SARTOR, *The right to be forgotten: dynamics of privacy and publicity*, in L. FLORIDI, *The protection of information and the right to privacy* (2014), Springer, p. 1-15. V. retro in questo volume il commento di G. FINOCCHIARO,

pubblicazione di informazioni vere su eventi passati¹⁰. È vero che alcuni precedenti e testi legislativi sembrano attribuire un diritto all'oblio su alcuni fatti del passato (per esempio reati giovanili¹¹), ma essi sono stati superati dalla costante giurisprudenza della Corte Suprema che ha affermato il primato della libertà di espressione. Ad esempio, nel caso *Cox v. Cohn* (429 US 469, 493-496 [1975]), concernente la pubblicazione del nome della vittima di uno stupro, la Corte Suprema affermava che, in generale, nessuna responsabilità poteva discendere dalla divulgazione di informazioni contenute in documenti pubblici. Il fatto che notizie vere siano pregiudizievoli alla reputazione dell'interessato non esclude la liceità della loro pubblicazione¹². Per i giudici statunitensi la pubblicazione della fedina penale di una persona è garantita dal Primo Emendamento. Secondo il diritto statunitense Wikipedia può legittimamente respingere la richiesta, presentata da due cittadini tedeschi, condannati per aver ucciso un attore famoso, che i loro nomi fossero rimossi dalla pagina su questo attore¹³.

La preminenza attribuita alla libertà di espressione ha inoltre condotto i giudici statunitensi, nella loro interpretazione della sezione 230 del Communication Decency Act, a riconoscere la più ampia tutela al provider che ospiti informazioni accessibili al pubblico, anche quando la distribuzione di tali informazioni un comportamento illecito da parte di chi le carica in rete. Ogni limitazione dell'immunità del provider comporterebbe infatti il rischio di una «censura collaterale» limitatrice della libertà di espressione, poiché il timore di incorrere in sanzioni indurrebbe il provider a rimuovere anche informazioni lecite, nel timore che possano esporlo a responsabilità¹⁴. Anche la libertà d'iniziativa economica

par. 2 e *infra* il commento di S.SICA e V.D'ANTONIO, par. 7.

¹⁰ F.WERRO, *The right to inform v. the right to be forgotten: A transatlantic clash*, in A.COLOMBI CIACCHI, C. GODT, P. ROTT, e L.J.SMITH (a cura di), *Liability in the Third Millennium*, pp. 285-300, Baden-Baden, 2009.

¹¹ La dottrina fa riferimento ad un caso del 1931 deciso dalla Corte d'Appello della California (*Melvin vs Reid*), in cui il diritto all'oblio è stato esplicitamente riconosciuto come una conseguenza immediata del diritto alla *privacy*. R.A.DOTTI, *Proteção da vida privada e liberdade de informação* (1980), São Paulo: Revista dos Tribunais, pp. 90-91.

¹² J.ROSEN, *The Right To Be Forgotten* (2012), Symposium Issue, 64 *Stan. L. Rev. Online* 88, February 13, p. 91.

¹³ *Ibid.* p. 88.

¹⁴ Sull'idea di censura collaterale, v., J.M.BALKIN, *The future of free expression in a digital age* (2008), *Pepperdine Law Review*, 36:101-18 e J.ROSEN, *The right to be forgotten* (2012), *Stanford Law Review Online*, 64:88-92. Per una generale limitazione della responsabilità del provider ai casi in cui si provi l'«actual malice» dello stesso, v. M.A.LEMLEY, *Rationalising Internet safe harbours* (2007), *Journal on Telecommunication*

viene spesso ad acquistare preminenza rispetto alla *privacy* nel contesto statunitense. Così la rilevazione e la cessione di profili di consumatori, la distribuzione di rapporti attinenti al credito, il riuso di dati personali per scopi diversi e ulteriori rispetto a quelli che ne hanno determinato la raccolta, sono ritenuti comportamenti leciti indipendentemente dal consenso dell'interessato. I vantaggi economici che queste pratiche possono comportare, facilitando gli scambi e la libertà d'iniziativa economica degli operatori, superano di regola, nella prospettiva statunitense, le esigenze di tutela della *privacy*, se non in ambiti nei quali i rischi siano particolarmente evidenti, come nel trattamento dei dati genetici¹⁵. Peraltro, anche nel diritto dell'Unione le esigenze del traffico economico prevalgono in taluni casi sulla *privacy*, consentendo, per ragioni economiche, trattamenti non autorizzati dall'interessato.

Ciò vale in particolare nell'ambito della formazione e dell'adempimento dei contratti, nella distribuzione d'informazioni sul credito, nella raccolta di informazioni per la tutela giudiziale di diritti anche economici, ecc.

Le due culture giuridiche sembrano differire anche nell'attitudine rispetto al rischio derivante dall'innovazione tecnologica. All'idea statunitense che l'innovazione debba essere libera e non debba richiedere autorizzazioni (*permissionless innovation*, secondo lo slogan di Vinton Cerf, uno degli inventori di Internet¹⁶), si oppone spesso in Europa il principio di precauzione, chiamato «legge della paura» dai suoi detrattori¹⁷, che assume la pericolosità e quindi l'illiceità dell'innovazione in assenza di prova contraria, verificata dall'autorità competente. Un esempio di questo atteggiamento può forse ravvisarsi nell'Art. 24, comma 1, lettera (g) del nostro Codice *privacy*. Anziché limitarsi ad affermare la liceità dei trattamenti destinati a soddisfare un legittimo interesse del titolare, in assenza di prevalente interesse contrario, come fa la Direttiva europea sulla protezione dei dati, la nostra legge richiede altresì la previsione della liceità del tratta-

and High Technology Law, 6:101-19. Sul rapporto tra tutela della *privacy* e responsabilità dei provider, vedi G.Sartor, *Providers' liabilities in the new EU data protection regulation: A threat to Internet freedoms?* (2013), *International Data Privacy Law*, pp. 3-12. V. anche G.Sartor e M.Viola De Azevedo Cunha, *Il caso Google-ViviDown tra protezione dei dati e libertà di espressione online*, in *Dir. Inf.* 2010, 645.

¹⁵ Il conflitto tra la tutela della *privacy* e l'esigenza di facilitare gli scambi mettendo a disposizione delle parti tutte le informazioni rilevanti era già sottolineata da S.Rodotà, *Tecnologie e diritti* (1995), Bologna.

¹⁶ V.CERF, *Keep the Internet open*, New York Times, 24 Maggio 2012.

¹⁷ Secondo la celebre caratterizzazione di C.SUNSTEIN, *Laws of fear: Beyond the precautionary principle* (2005), Cambridge University Press.

mento da parte del Garante, rendendo così illegittimo ogni trattamento di dati personali che non sia previsto dal garante o espressamente consentito dal titolare. La possibilità di elaborare dati personali in modi nuovi, per scopi legittimi, ma non originariamente previsti ed espressamente consentiti, è divenuta particolarmente significativa oggi, nel contesto del c.d. *big data*. Si tratta della raccolta automatica di enormi quantità di dati (sull'uso dei servizi di Internet, le abitudini dei consumatori, il traffico, ecc.) che possono essere utilizzati, grazie alle tecniche del c.d. *data mining*, per molteplici finalità di utilità economica, scientifica, o sociale, non prevedibili al momento della raccolta dei dati stessi¹⁸. Ai diversi valori giuridici, o meglio al diverso peso di essi nel sistema giuridico statunitense e in quello europeo, si aggiunge il diverso peso degli interessi in gioco. I protagonisti dell'economia della rete si trovano negli Stati Uniti, essi godono dei vantaggi economici dell'elaborazione dei dati personali, e hanno un'enorme capacità di lobbying nei confronti del legislatore statunitense. Non stupisce che sia proprio il legislatore statunitense a dedicare maggiore attenzione agli interessi dei protagonisti economici di Internet, o almeno a esitare di fronte a ogni misura che possa compromettere tali interessi. Il legislatore europeo invece, benché oggetto esso stesso di forti pressioni lobbistiche, sente l'esigenza di contribuire a limitare lo strapotere delle imprese statunitensi della new economy, a tutela dei consumatori, ma anche delle imprese europee, cosicché la restrizione delle pratiche commerciali che incidono sulla *privacy* può assumere connotazioni protezionistiche.

Anche nel campo pubblico e in particolare in quello della sicurezza, le culture giuridiche europee e statunitensi sembrano dare diverso peso agli interessi, valori, ed esigenze in gioco. Gli Stati Uniti, quale una superpotenza militare, impegnata in numerosi scenari, e quindi soggetta a particolari rischi e minacce, divenute realistiche dopo l'attentato alle Torri Gemelle, tendono a dare maggiore rilievo alle esigenze della sicurezza nazionale, così come a quelle strategiche e geopolitiche¹⁹. Inoltre, il fatto che gli Stati Uniti posseggano strumenti per il controllo delle comunica-

¹⁸ Quando i dati diventano una materia prima, suscettibile di usi molteplici, emerge l'esigenza di evitare lo 'spreco' che risulterebbe dall'eliminazione delle informazioni disponibili non appena raggiunto lo scopo della loro raccolta, esigenza in conflitto con i principi della minimizzazione dei dati personali e della loro utilizzabilità solo per scopi predeterminati. Questa tesi è sostenuta, tra gli altri da F.CATE, P.CULLEN e V.MAYER-SCHÖNBERGER, *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines* (2014), Microsoft Corporation.

¹⁹ Il ricorso a tecnologie di sorveglianza globale, quale mezzo necessario per anticipare minacce terroristiche è affermato da Ph.BOBITT, *The Shield of Achilles* (2002), Penguin; Ph.BOBITT, *Terror and Consent* (2008), Allen Lane.

zioni a livello globale, e che nel loro territorio risiedano i principali attori della rete, rende a essi possibile effettuare una raccolta ed analisi globale di informazioni, come evidenziato dal programma Prism, reso noto dalle rivelazioni di Edward Snowden²⁰. Quindi, la presenza di maggiori esigenze in tema di sicurezza e controllo globali, e la disponibilità di mezzi di controllo capaci di soddisfare in qualche misura tali esigenze, induce a una prospettiva più favorevole all'impiego di mezzi di sorveglianza. Ciò non significa che la raccolta massiccia di informazioni effettuata a tal fine possa considerarsi moralmente e politicamente giustificata, e legittima alla luce della stessa normativa americana e del diritto internazionale, ma contribuisce a spiegare come alla sorpresa e all'indignazione dei governi europei (siano esse autentiche o ipocrite) corrispondano atteggiamenti più sfumati e differenziati di là dall'Atlantico²¹. Le diversità che abbiamo illustrato contribuiscono a spiegare perché Stati Uniti e Unione europea abbiano adottato diversi modelli per la protezione dei dati, una disciplina generale in Europa e discipline settoriali, principalmente rivolte verso i soggetti pubblici, negli Stati Uniti. Ciò non esclude importanti convergenze. Ricordiamo come la disciplina Europea sulla protezione dei dati riprenda i *Fair Information Principles*, già enunciati in una relazione del *U.S. Secretary's Advisory Committee on Automated Personal Data Systems* nel 1973²², nell'ambito dell'iniziativa culminata nell'adozione del *Federal Privacy Act* statunitense nel 1974. Inoltre sempre più pressanti si fanno le richieste di una disciplina più rigorosa della *privacy* negli Stati Uniti, estesa anche al settore privato, e che possibilmente preveda anche un'autorità di controllo imparziale. Diverse soluzioni sono state proposte al fine di conciliare tale disciplina con la tradizione giuridica statunitense, dall'accentuazione degli aspetti proprietari della *privacy*, al rilievo delle norme sociali (*fair information rules*), all'affidare il controllo a una commissione parlamentare piuttosto che a un'autorità amministrativa²³.

Una convergenza verso una riduzione della tutela della *privacy* si è

²⁰ V. H.FARRELL e M.FINNEMORE, *The End of Hypocrisy: American Foreign Policy in the Age of Leaks* (2013), 92 *Foreign Aff.* 22.

²¹ Per una difesa della opportunità strategica e della legittimità giuridica di Prism, v. Ph.BOBBIT, *NSA is upholding, not subverting, the law* (2013). Il testo è disponibile a <http://www.ft.com/cms/s/0/2da229bc-d1bc-11e2-9336-00144feab7de.html#axzz39N5uZYM1> [consultato il 03/08/2014].

²² U.S.A., *Records, computers and the rights of citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, 1973, Il testo è disponibile all'indirizzo <https://www.hsdl.org/?view&did=479784> [consultato il 03/08/2014].

²³ Per quest'ultima tesi, si veda J.ROSEN, «*About the Author*». *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (2004). Random House pp. 213 ss..

invece realizzata dopo gli attacchi terroristici del settembre 2011²⁴. Gli Stati Uniti, subito dopo gli attentati alle Torri Gemelle, adottavano due provvedimenti restrittivi dei diritti dei cittadini. Il Patriot Act (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*) autorizza agenzie ed enti governativi ad avere libero accesso a varie banche di dati pubbliche e private²⁵, permettendo, ad esempio, l'accesso alla cronologia delle chiamate telefoniche, e-mail e a file finanziari e medici. L'*Aviation and Transportation Security Act* esige che tutte le compagnie aeree che volano verso gli Stati Uniti forniscano i dati dei propri passeggeri (*Passenger Name Record* - PNR) al *Customs and Border Protection Administration* degli Stati Uniti (CBP) prima che l'aereo decolli verso gli USA. Anche nell'Unione Europea l'idea che la *privacy* e la protezione dei dati possano essere limitate ai fini della lotta contro il terrorismo e la criminalità ha ottenuto il sostegno di molti governi, soprattutto dopo gli attentati terroristici di Madrid e Londra. Lo scambio di dati personali tra le autorità di polizia in diversi Stati membri dell'UE è diventato elemento essenziale della cooperazione internazionale contro il terrorismo e la criminalità organizzata²⁶. Recentemente, tuttavia, l'esigenza della protezione dei dati, anche nel campo sicurezza, si è imposta nella giurisprudenza della Corte di Giustizia, che ha dichiarato l'illegittimità della Direttiva sulla Data Retention, che imponeva ai provider di servizi di telecomunicazione la conservazione dei dati sul traffico telefonico²⁷. Già il Gruppo di Lavoro Articolo 29 nel suo «Parere sulla necessità di un approccio equilibrato alla lotta contro il terrorismo», aveva espresso perplessità su tale provvedimento, affermando che «I provvedimenti contro il terrorismo non devono compromettere gli standard per la

²⁴ S. RODOTÀ, *La vita e le regole – Tra diritto e non diritto* (2006), Milano: Feltrinelli, p. 82. «La prospettiva di una più forte tutela attraverso strumenti giuridici, tuttavia, è contraddetta dalle tendenze legislative avviate dopo gli attentati dell'11 settembre 2001. Negli Stati Uniti, il Patriot Act consente a una serie di soggetti pubblici un accesso pieno a qualsiasi banca dati pubblica o private, cancellando così la garanzia offerta dai divieti di interconnessione. Diventa problematica la possibilità di sottrarre il corpo elettronico allo sguardo totale di poteri non controllabili».

²⁵ S. RODOTÀ *La vita e le regole ecc.* (2005), *op. cit.* p. 82.

²⁶ Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen (COM(2009)0262 final). [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0262:EN:HTML\[consultato il 03/08/2014\]..](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0262:EN:HTML[consultato il 03/08/2014]..)

²⁷ DIRETTIVA 2006/24/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

protezione dei diritti fondamentali che caratterizzano le società democratiche, e non è necessario che producano ‘effetti siffatti’ e rilevando che «un elemento fondamentale della lotta al terrorismo è costituito dall’impegno alla salvaguardia di quei valori fondamentali che costituiscono la base di ogni società democratica, ossia proprio i valori che coloro che praticano l’uso della violenza tentano di distruggere»²⁸. Tuttavia, a conferma della diversità delle prospettive culturali e politiche presenti in Europa, il governo del Regno Unito ha recentemente presentato una proposta di legge, con il sostegno di maggioranza e opposizione, che reintroduce l’obbligo di conservare i dati sul traffico telefonico, in vista del loro uso nella prevenzione e repressione del terrorismo e della criminalità²⁹. Nel Sudamerica, la protezione dei dati personali è ispirata alla prospettiva europea³⁰, a causa dei legami storici e culturali tra Europa continentale e Sudamerica, che si estendono alla cultura giuridica e al disegno istituzionale. Anche nel Sudamerica la protezione della *privacy* si collega al principio del rispetto della dignità e la maggior parte dei paesi sudamericani ha riconosciuto l’*Habeas Data* quale diritto costituzionalmente garantito. Molti paesi (circa la metà) hanno già adottato una disciplina generale di protezione dei dati personali ispirata al modello europeo, anche per poter soddisfare il requisito di adeguatezza di cui all’articolo 25 della direttiva europea 95/46/CE, e quindi poter elaborare dati provenienti dall’Europa. Peraltro, il Brasile, la più grande economia del Sudamerica, benché abbia assunto la leadership regionale nella protezione dei dati dopo le rivelazioni del caso Snowden, non dispone ancora di una legge generale sulla protezione dei dati.

Il Sudamerica sembra propendere per la prospettiva europea anche sul diritto all’oblio, benché non manchino decisioni giudiziarie e scelte legislative maggiormente sensibili alle esigenze della libertà di espressione e della protezione degli intermediari. In Argentina, paese che ha adottato una legge generale sulla protezione dei dati ispirata dalla direttiva europea,

²⁸ ARTICOLO 29 - GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI. Parere 10/2001 sulla necessità di un approccio equilibrato alla lotta contro il terrorismo. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wrp53_it.pdf#h2-14 [consultato il 30/06/2014]..

²⁹ UK Data Retention and Investigatory Powers Act 2014. Il testo è disponibile a http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf [consultato il 03/08/2014].

³⁰ A.M.LEIVA, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches* (2012), *International Law News*, Vol. 41, n° 4. Il testo è disponibile a http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_america_survey_legal_approaches.html [consultato il 30/06/2014].

un recente caso ha affrontato il diritto all'oblio. Una pop star argentina, che aveva posato per delle foto osé in gioventù, aveva chiesto a Google e Yahoo di escludere le foto dalle loro ricerche, sostenendo che la loro reperibilità avrebbe violato il suo diritto all'oblio. Il giudice argentino si schierava con la pop star, condannando Google e Yahoo a pagare una multa, e ordinando loro di rimuovere tutte le immagini sessuali che contenevano il nome della pop star. La decisione era però ribaltata in appello, considerando che Google e Yahoo avrebbero potuto essere ritenute responsabili solo se avessero saputo che il contenuto era diffamatorio e avessero avuto la possibilità di rimuoverlo. Ci sono oggi almeno centotrenta casi pendenti nei tribunali argentini nei quali si chiede la rimozione di foto e contenuti generati dagli utenti, la maggior parte promossi da personaggi dello spettacolo³¹.

In Brasile, il *Superior Tribunal de Justiça* – La Corte d'appello più alta in Brasile per questioni non-costituzionali del diritto federale – ha recentemente affrontato in due casi (congiuntamente decisi il 28 maggio 2013) il tema diritto all'oblio nei confronti dei provider. Nel primo caso i giudici brasiliani riconoscevano il diritto alla rimozione della notizia concernente l'incriminazione di un soggetto poi assolto. Secondo la corte la continuata pubblicazione della notizia avrebbe violato la dignità umana dell'interessato, che continuava a essere considerato un 'sospetto' nel suo ambiente sociale³². Nel secondo caso³³, la Corte respingeva la richiesta che il nome della vittima di un omicidio risalente al 1958 non fosse menzionato in un programma televisivo. La Corte riteneva che il reato avesse avuto notorietà nazionale e che il nome della vittima fosse diventato parte della memoria collettiva, e quindi fosse necessario alla rappresentazione dell'evento.

In Brasile la recente legge sul *Marco Civil* garantisce l'immunità dei fornitori di servizi di Internet, i quali sono responsabili per la diffusione di informazioni illegali solo se non adempiono a ordini di rimozione di un'autorità competente (un giudice)³⁴. Pertanto, sembra che in Brasile il provider non sia tenuto a conformarsi a richieste di rimozione da parte di privati, in assenza di previa determinazione autoritativa circa l'esistenza di

³¹ J.ROSEN (2012), *The Right To Be Forgotten ecc. op. cit.* p. 91.

³² Superior Tribunal de Justiça. REsp 1.334.097-RJ, Rel. Min. Luis Felipe Salomão.

³³ Superior Tribunal de Justiça. REsp 1.335.153-RJ, Rel. Min. Luis Felipe Salomão.

³⁴ Articolo 19. Al fine di garantire la libertà di espressione e di evitare la censura, il fornitore di servizi di Internet sono responsabili solo se non rispettano una decisione di una autorità giudiziaria nel senso di escludere tale contenuto entro i limiti tecnici del loro servizio e entro il termine indicato nella decisione, fatte salve le disposizioni di legge in senso contrario.

un obbligo di rimozione. L'unica eccezione è il caso di immagini, video o altri materiali contenenti nudità o atti sessuali di carattere privato, nel quale caso il provider dovrà conformarsi alla richiesta di rimozione da parte dell'interessato. Nelle pagine seguenti considereremo alcuni casi in cui si sono manifestate queste convergenze e divergenze tra Europa, Stati Uniti e Sudamerica, per poi approfondire l'esame dei contrasti emersi rispetto al caso Google-Spain e trarre alcune considerazioni conclusive.

2. La trasmissione dei dati sui passeggeri (PNR) e gli accordi SWIFT³⁵

Lo *US Aviation and Transportation Security Act*, adottato nel 2001, esigeva che tutte le compagnie aeree che volano verso gli Stati Uniti fornissero i dati dei propri passeggeri, detti PNR, (*Passenger Name Records*). Tale norma dava luogo a reazioni accese in alcuni Stati membri dell'UE, che conducevano a negoziati tra l'UE e gli Stati Uniti con l'obiettivo di consentire la trasmissione dei PNR, assicurando un livello adeguato di protezione dei dati. Nel febbraio 2003 la Commissione Europea e la *customs and Border Protection Administration (CBP)* emettevano una dichiarazione congiunta³⁶ in base alla quale la Commissione autorizzava temporaneamente le compagnie aeree europee a trasferire i PNR alle autorità statunitensi, in attesa di trovare una soluzione definitiva al problema.

Nel marzo del 2004 la Commissione sottoponeva al Parlamento il progetto della propria decisione sull'adeguatezza del trattamento dei PRN rispetto agli standard europei, accompagnato dal progetto d'impegno del CBP, cui faceva seguito la proposta di decisione del Consiglio concernente un accordo con gli Stati Uniti.

Nonostante le osservazioni critiche del Parlamento, la Commissione e il Consiglio procedevano adottando rispettivamente la decisione di adeguatezza e l'accordo. Il Parlamento ricorreva alla Corte di Giustizia contro i due provvedimenti, adducendo diversi motivi: eccesso di potere, violazione dei principi essenziali della direttiva, violazione dei diritti fondamentali e violazione del principio di proporzionalità.

Il 30 maggio 2006 la Corte di Giustizia annullava i provvedimenti

³⁵ V. M.BOTTA e M.VIOLA DE AZEVEDO CUNHA, *La protezione dei dati personali nelle relazioni tra UE e USA: le negoziazioni sui trasferimento dei PNR*, in *Dir.Inf.*, 2010, pp. 315-341.

³⁶ *Joint statement* approvato al termine della riunione tenutasi a Bruxelles il 17/18 febbraio 2003 tra i rappresentanti della Commissione Europea e del CBP.

impugnati sulla base del primo motivo, cioè, in ragione fatto che il trattamento verteva su questioni di pubblica sicurezza, e pertanto non rientrava nella disciplina comunitaria sulla protezione dei dati, ragion per cui né la Commissione poteva deliberarne l'adeguatezza né il Consiglio, quale organo delle Comunità Europee, poteva regolarlo mediante l'accordo con gli USA. Gli USA e l'Unione Europea adottavano allora un accordo temporaneo («*interim agreement*»³⁷), per permettere la continuazione del trasferimento dei PNR agli USA in attesa dell'accordo definitivo. Nel 2007 si stipulava un nuovo accordo, che consentiva un più ampio trattamento dei PNR, in ragione delle pressioni effettuate dal Dipartimento della sicurezza interna statunitense sulla Presidenza del Consiglio e la Commissione Europea. Tale accordo era adottato dal Consiglio quale organo del terzo pilastro dell'unione Europea (Cooperazione giudiziaria e di polizia in materia penale) e quindi non era soggetto al controllo della Corte di Giustizia.

Nel 2011, l'Unione Europea, quale istituzione che riuniva le competenze precedentemente suddivise nei c.d. Pilastri, firmava un nuovo accordo PNR con gli Stati Uniti. Tale accordo è entrato in vigore il 1 Luglio 2012 con il consenso del Parlamento europeo e l'approvazione del Consiglio dell'UE³⁸. L'accordo prevede alcune garanzie a protezione dei dati, giudicate peraltro insufficienti dal Gruppo di Lavoro Articolo 29³⁹. In Sudamerica, i dati PNR sono generalmente trasferiti alle autorità statunitensi senza che siano ancora stati stipulati, per quanto è noto, accordi internazionali in materia. In particolare, il governo brasiliano nel 2005 annunciava di aver autorizzato le compagnie aeree a fornire alle autorità statunitensi i dati dei passeggeri e di aver iniziato i negoziati

³⁷ Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security. Firmato a Washington il 19.10.2006. Il testo dell'accordo è disponibile a: http://ec.europa.eu/justice_homelfsj/privacy/docs/adequacy/pnr/2006_10_accord_US_en.pdf [consultato il 03/08/2014].

³⁸ COUNCIL OF THE EUROPEAN UNION. Council adopts new EU-US agreement on Passenger Name Records (PNR). Luxembourg, 26 April 2012 - 9186/12. Il testo è disponibile a http://consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf. [consultato il 05/07/2014].

³⁹ ARTICLE 29 WORKING PARTY. Letter from the Article 29 Working Party addressed to LIBE Committee of the European Parliament regarding the new draft agreement on the transfer and use of Passenger Name Records, known as PNR data. Brussels, 6 January 2012. Il testo è disponibile a http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf [consultato il 14/08/2014].

con il governo degli Stati Uniti in vista della conclusione di un accordo PNR Brasile – USA⁴⁰. Gli accordi sul trasferimento dei PNR evidenziano come esigenze di sicurezza possano condurre a limitazioni della *privacy* e della protezione dei dati. Queste esigenze, oltre che le pressioni politiche statunitensi, hanno indotto l'Unione a conformarsi alle richieste di trasferimento, anche se il compromesso emerso non ha pienamente soddisfatto i difensori della *privacy*, e in particolare le stesse Autorità europee per la protezione dei dati. Gli accessi al database delle operazioni interbancarie SWIFT (*Society for Worldwide Interbank Financial Telecommunication*), accessi effettuati dal governo statunitense nell'ambito del programma anti-terrorismo TFTP (*Terrorist Finance Tracking Program*), hanno originato un analogo conflitto tra Stati Uniti e Unione Europea. Anche in questo caso una prima bozza di trattato per l'accesso ai dati SWIFT, frutto dei negoziati tra Stati Uniti e Commissione, era respinta dal Parlamento Europeo, che approvava poi una versione successiva, che aggiungeva alcune garanzie a tutela della *privacy* dei cittadini europei. Per assicurare una più efficace garanzia dei dati europei si adottava altresì una misura tecnologica: l'architettura del sistema informatico di Swift era modificata, in modo che i dati concernenti le operazioni intraeuropee rimanessero esclusivamente in Europa, non essendo più riportati nel centro dati statunitense di SWIFT.

Le rivelazioni di Edward Snowden, evidenziavano peraltro come gli Stati Uniti avessero violato o eluso i limiti sull'uso dei dati stabiliti dall'accordo. Di conseguenza il Parlamento Europeo chiedeva nel 2013 la revoca del trattato⁴¹.

3. Il caso Snowden

Come già osservato nella prima sezione di questo articolo, i principali ISP e fornitori di servizi di rete sono basati negli Stati Uniti. La preminenza economica delle imprese statunitensi ha implicazioni politiche importanti, poiché tali imprese sono in grado di determinare, in modo confor-

⁴⁰ 'O Globo'. O mundo. «Governo brasileiro aceita compartilhar informações de passageiros com destino aos Estados Unidos». Pubblicato nel 26 febbraio 2005.

⁴¹ PARLAMENTO EUROPEO. Risoluzione del Parlamento europeo del 23 ottobre 2013 sulla sospensione dell'accordo TFTP a seguito della sorveglianza dell'Agenzia per la sicurezza nazionale statunitense (2013/2831(RSP)). Il testo è disponibile a <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+V0//IT> [consultato il 14/08/2014].

me ai propri interessi e a valori, la regolazione di Internet. Possono farlo predisponendo unilateralmente le modalità di funzionamento dei propri servizi e le regole cui gli utenti si debbono attenere, ma anche influenzando la definizione di standard tecnici o esercitando pressioni nei confronti dei decisori politici. Il ruolo politico di tali imprese è rafforzato dalla posizione tendenzialmente monopolistica di cui godono, grazie all'effetto di rete (l'attrattività delle reti più ampie), posizione che offre loro grandi spazi di azione, anche in contrasto agli interessi degli utenti. Inoltre, il fatto che i protagonisti di Internet siano situati negli Stati Uniti conferisce una posizione privilegiata al governo di questo paese, alla cui giurisdizione sono sottoposte tali imprese. Le imprese di Internet possono essere indotte o costrette a collaborare con il governo statunitense, fornendo a tale governo dati e strumenti per operazioni di sorveglianza sul terrorismo, ma anche per indagini giudiziarie, spionaggio militare e politico, e persino spionaggio industriale. È opportuno ricordare che le istituzioni economiche e politiche statunitensi, e i valori che le ispirano, hanno contribuito in modo decisivo allo sviluppo di Internet quale ambito di progresso e libertà. In particolare, le libertà garantite in questo paese all'iniziativa economica privata, così come alla ricerca scientifica e alla manifestazione di opinioni, accompagnate dal sostegno pubblico alle iniziative tecnologiche, hanno consentito che Internet nascesse quale rete aperta, si arricchisse di sempre nuove funzionalità e diventasse globale, conservando la capacità di favorire l'innovazione delle tecnologie e dei modelli economici, ma anche la creatività degli individui, e il dialogo politico e culturale⁴².

Le rivelazioni dall'ex consulente della NSA (*National Security Agency* statunitense), Edward Snowden – l'esistenza di programmi di sorveglianza di massa, che contavano anche sulla complicità di altri paesi occidentali⁴³ – hanno però messo in luce il lato 'oscuro' del predominio statunitense sulla rete. Nel fatto che «gli Stati Uniti controllano Internet, le aziende americane profitano sproporzionatamente di Internet, i servizi di sicurezza statunitensi hanno accesso privilegiato a tutto che attraversa Internet» si è ravvisata una nuova forma di colonialismo, in cui si fondono profili economici e politici⁴⁴. Tali rivelazioni hanno messo in discussione la

⁴² Sulla 'generatività' di Internet, v. J. ZITTRAIN, *The Generative Internet* (2006), 119 *Harvard Law Review* 1974.

⁴³ M. SHEARS, *Snowden and the Politics of Internet Governance* (2014). Security & Surveillance. Il testo è disponibile a <https://cdt.org/blog/snowden-and-the-politics-of-internet-governance/> (03/08/2014).

⁴⁴ Dichiarazioni attribuite a P. Verveer da R. HILL, *Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means?*, in R. RADU et al. (eds), *The Evolution of*

governance di Internet, oggi svolta attraverso organizzazioni private create in base alle leggi degli Stati Uniti e situate nel territorio degli Stati Uniti (ICANN e IETF), grazie alle quali gli Stati Uniti possono esercitare un'influenza anche sulle norme tecniche di funzionamento di Internet e sulla sua amministrazione.

Sulla scia del caso Snowden, numerosi governi hanno sostenuto, con diverse motivazioni, l'esigenza di passare a un nuovo ordine multilaterale. Come esempio si può citare la dichiarazione presentata dal governo del Pakistan – con il sostegno Ecuador, Venezuela, Cuba, Zimbabwe, Uganda, Russia, Indonesia, Bolivia, Iran e Cina – al Consiglio per i Diritti Umani nel settembre 2013, concernente le rivelazioni di Snowden, il fallimento dell'attuale sistema di governance di Internet e la necessità di un nuovo quadro internazionale⁴⁵. Benché si possa dubitare della misura in cui tali richieste esprimano l'esigenza di una maggiore tutela dei diritti umani, piuttosto che quella di sottoporre Internet a un più intenso controllo politico finalizzato alla repressione del dissenso, il predominio statunitense su Internet sembra insostenibile a lungo termine, e vi è l'esigenza di trovare un diverso quadro istituzionale per il governo di questa infrastruttura globale.

In Europa, Germania, Francia e Spagna, hanno reagito con indignazione alle rivelazioni del monitoraggio di massa effettuato dalla NSA. In Germania l'opinione pubblica e i partiti di opposizione hanno chiesto spiegazioni al governo, il quale ha risposto assumendo un ruolo di leadership nella contestazione le pratiche di sorveglianza e spionaggio statunitensi. Il governo tedesco è giunto a proporre agli Stati Uniti di firmare un trattato bilaterale di non spionaggio, pur ribadendo che gli Stati Uniti rimanevano un partner fondamentale per la Germania e che, in particolare, che i negoziati del TTIP (*Transatlantic Trade and Investment Partnership*) non erano in discussione⁴⁶.

Nonostante l'apparente indignata sorpresa di alcuni capi di stato europei, emergeva successivamente, con il rilascio di nuovi documenti da parte dello stesso Snowden, che alcuni paesi europei, tra cui Francia e Regno Unito, avevano agito di concerto con la NSA nelle pratiche di sorveglianza globale e avevano condiviso con gli Stati Uniti enormi quantità di dati⁴⁷.

Global Internet Governance: Principles and Policies in the Making, Springer and Schulthess, 2014, p. 81.

⁴⁵ M. SHEARS, *Snowden and the Politics ecc.* (2014). *op. cit.*

⁴⁶ V. <http://rt.com/news/170868-merkel-spy-scandal-serious/> [consultato il 03/08/2014].

⁴⁷ J. FOLLOROU, *La France, précieux partenaire de l'espionnage de la NSA* (2014), Le Monde. Disponibile a <http://www.lemonde.fr/technologies/article/2013/11/29/la-france-precieux-partie->

Il Direttore nazionale dell'intelligence USA, James Clapper, dichiarava, infatti, al Congresso degli Stati Uniti che lo stupore dei governi europei era almeno in parte ipocrita, poiché la sorveglianza era stata compiuta con il sostegno delle agenzie d'intelligence locali⁴⁸.

Anche in America Latina le reazioni alle rivelazioni di Snowden erano forti, soprattutto dopo che la stampa aveva reso noto che gli Stati Uniti stavano conducendo operazioni di spionaggio in diversi paesi sudamericani, tra cui Brasile, Colombia, Messico e Venezuela.

In particolare, tali operazioni non si limitavano alla prevenzione del terrorismo e della criminalità, ma si estendevano al controllo di Internet e delle comunicazioni telefoniche con finalità commerciali, per esempio, per cercare informazioni sull'industria petrolifera⁴⁹. Questa situazione portava la Presidente del Brasile – che, come la Cancelliera tedesca, è stata oggetto di sorveglianza da parte dei servizi statunitensi – ad affermare al vertice del Mercosur del 12 luglio 2013 che «qualsiasi atto di spionaggio che violi i diritti umani, soprattutto il fondamentale diritto alla *privacy*, e minacci la sovranità delle nazioni, merita di essere condannato da qualsiasi paese che si definisca come democratico⁵⁰». Le rivelazioni di Snowden portavano la Presidente del Brasile a cancellare un viaggio negli Stati Uniti nel mese di ottobre 2013 e ad accelerare l'emanazione del c.d. «Marco Internet Civil, la legge che «stabilisce principi, garanzie, diritti e obblighi per l'uso dell'Internet in Brasile» (Legge n 12,965, del 23 aprile 2014⁵¹). A conferma del ruolo di leadership assunto dalla Germania e dal Brasile nelle rispettive aree d'influenza – Unione Europea e America Latina - Brasile e Germania presentavano una proposta di risoluzione comune sulla *privacy* online nell'Assemblea generale delle Nazioni Unite, che era approvata all'unanimità⁵². Di conseguenza, l'Assemblea generale delle Nazioni Unite chiedeva all'Alto commissario per i diritti umani di preparare una relazione sul diritto alla *privacy* nell'era digitale.

[naire-de-l-espionnage-de-la-nsa_3522653_651865.html](http://www.nsa.gov/press/2013/07/13/naire-de-l-espionnage-de-la-nsa_3522653_651865.html) [consultato il 03/08/2014].

⁴⁸ J. BORGER, *GCHQ and European spy agencies worked together on mass surveillance* (2014). The Guardian. Disponibile a <http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden> [consultato il 03/08/2014].

⁴⁹ V. Latin America and Edward Snowden: South Americans in glasshouses. The Economist. Disponibile a <http://www.economist.com/node/21582154/print> [consultato il 03/08/2014].

⁵⁰ V. Latin America and Edward Snowden: South Americans in glasshouses. Cit.

⁵¹ Il testo della legge è disponibile (in portoghese) a http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm [consultato il 03/08/2014].

⁵² United Nations General Assembly. Resolution 68/167 on The right to *privacy* in the digital age. Adopted on 18 December 2013. Il testo è disponibile a http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167. [consultato il 05/06/2014].

4. La discussione sul regolamento sulla protezione dei dati

La Proposta della commissione per un Regolamento Generale sulla Protezione dei Dati Personali ha suscitato ampie discussioni tra l'Unione da un lato e le imprese di Internet e il governo statunitense dall'altro, dibattito che ha risentito delle rivelazioni di Snowden⁵³. Alcuni aspetti del regolamento rispondono alle esigenze delle imprese globali di Internet: la sostituzione di un'unica normativa europea alle diverse discipline nazionali oggi esistenti; l'indicazione di un'unica autorità per la protezione dei dati quale soggetto competente per tutte le questioni concernenti un certo titolare, quella dove è stabilito il titolare stesso; la creazione di un organo di appello per assicurare la coerenza tra le decisioni nazionali⁵⁴; l'esplicita estensione delle immunità dei provider anche alle violazioni della protezione dei dati; la possibilità che l'adozione unilaterale di regole vincolanti sulla protezione dei dati da parte di un'impresa stabilita in un paese estero possa costituire una base giuridica sufficiente al trattamento dei dati anche in mancanza di un'adeguata disciplina autoritativa. Adottando il modello tipicamente statunitense dell'autoregolamentazione, il Parlamento europeo ha introdotto nella bozza predisposta dalla Commissione il sigillo europeo per la protezione dei dati, rilasciato dalle autorità di protezione dei dati per garantire che il titolare o il responsabile è in conformità al regolamento (art. 43). Il sigillo limita la responsabilità amministrativa dei titolari, e consente loro di trasferire dati all'estero senza dover ottenere volta per volta l'autorizzazione delle autorità di protezione dei dati⁵⁵. Altri aspetti del regolamento, invece, hanno incontrato l'opposizione delle imprese e del governo statunitensi: la previsione di regole tecniche per la *privacy by design* stabilite dalla commissione, anziché da organizzazioni per la standardizzazione aperte e basate sulla partecipazione di tutte gli interessati (multi-stakeholderism); l'eccessivo rigore degli obblighi di

⁵³ C.KUNER et al., *The proposed EU data protection regulation two years later* (2014). *Privacy & Security Law Report*, 13 PVLR 8. Bureau of National Affairs, p. 1.

⁵⁴ Nel Consiglio dell'Unione europea, peraltro, sono emersi profondi disaccordi circa la competenza unica (one-stop shop) e il meccanismo di appello. Così osservano KUNER et al. (2014), *The proposed ecc. op. cit.*, p. 6: Diversi blocchi di stati membri hanno opinioni contrastanti in merito al regolamento: alcuni vogliono raggiungere presto un accordo su di esso (ad esempio, Francia, Italia e Spagna), altri sono completamente opposti (ad esempio, in Danimarca, Svezia e Regno Unito), e il terzo gruppo sta nel mezzo. La posizione assunta dalla Germania sarà fondamentale per vedere se il Consiglio possa raggiungere un accordo".

⁵⁵ C.KUNER et al *The proposed ecc.* (2014), *op. cit.*, p. 3.

notifica di 'data breaches' (poi attenuati nelle modifiche introdotte dal Parlamento); la potenziale applicabilità della normativa europea a ogni trattamento che coinvolga interessati situati in Europa anche quando il sito che esegue il trattamento non abbia specifica destinazione europea⁵⁶. Il tema più controverso è stato però quello del diritto all'oblio, o del 'diritto a essere dimenticati', la cui portata innovativa era stata enfatizzata dalla Commissaria Reding. Nonostante le affermazioni rassicuranti della stessa Reding e della Commissione, secondo cui tale diritto non avrebbe limitato le libertà di espressione, informazione e ricerca storica⁵⁷, il possibile conflitto era immediatamente identificato ed enfatizzato dagli osservatori statunitensi. Secondo l'opinione prevalente negli Stati Uniti, l'affermazione di un diritto dell'interessato alla rimozione delle informazioni che lo riguardano metterebbe a rischio le libertà altrui, e in particolare le libertà di esprimere opinioni su terzi, di comunicare informazioni, e di accedere alle stesse. Le potenzialità censorie di tale diritto erano addirittura assimilate agli interventi su Internet attuati da regimi oppressivi, come la Cina e alcuni governi del Medio Oriente⁵⁸, e si affermava che la disciplina del 'diritto ad essere dimenticati', imponendo a Google di rispondere alle richieste di rimozione, avrebbe trasformato Google stessa in un riluttante «censore capo per l'Unione europea⁵⁹». Peter Fleisch, Global Privacy Council di Google, paventava l'adozione di un'«interpretazione estremistica» del «right to be forgotten», secondo la quale gli interessati non solo avrebbero potuto chiedere alle autorità competenti di ordinare la rimozione ai fornitori dei contenuti, ma si sarebbero potuti rivolgere direttamente agli intermediari di Internet, chiedendo loro di rimuovere informazioni personali, e gli intermediari sarebbero stati responsabili se si fossero rifiutati di ottemperare nei casi in cui l'informazione avrebbe invece dovuto essere rimossa (secondo il successivo giudizio dell'autorità competente⁶⁰).

⁵⁶ V. <http://www.insideprivacy.com/international/european-union/draft-report-on-the-proposed-eu-data-protection-regulation-released/> [consultato il 14/08/2014].

⁵⁷ V. REDING, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age* 5 (22/01/2012). Disponibile a <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF> [consultato il 15/08/2014].

⁵⁸ J. ROSEN, *The Delete Squad Google, Twitter, Facebook and the new global battle over the future of free speech* (2013), *The New Republic*, (April 29): pp. 1-7.

⁵⁹ J. ROSEN, *The right to be forgotten* (2012). *Stanford Law Review Online*, pp. 64:88-92.

⁶⁰ V. anche P. Korenhof et al., *Timing the Right to Be Forgotten: A study into «time» as a factor in deciding about retention or erasure of data* (2004). Paper written by panelists of the «Timing the Right to Be Forgotten» panel at the Computers, Privacy and Data Protection Conference 2014 Panel organized by Paulan Korenhof and the Tilburg Institute for Law, Technology, and Society TILT); G. Sartor, *The right to be forgotten:*

Queste osservazioni critiche erano accolte in qualche misura dal Parlamento Europeo, il quale, modificava il testo predisposto dalla Commissione, eliminando il riferimento a un «right to be forgotten» sostituito dal richiamo del tradizionale diritto alla cancellazione (erasure) di dati elaborati senza una base giuridica⁶¹. Il Parlamento introduceva altresì tra le condizioni per la cancellazione la presenza di una decisione «final and absolute» di una «court or regulatory authority» suggerendo forse come il giudizio di illegittimità, presupposto per la cancellazione, dovesse essere affidato ad autorità pubbliche competenti, piuttosto che agli intermediari.

Questo apparente avvicinamento tra posizioni europee e statunitensi sulla rimozione di informazioni da Internet era però interrotto dalla decisione della Corte di Giustizia sul caso Google-Spain, che adottava proprio l'interpretazione qualificata come 'estremistica' dal general legal counsel di Google, Peter Fleischer. I giudici, infatti, conferiscono all'interessato il diritto rimozione di link a notizie legittimamente pubblicate e distribuite in rete, un diritto esercitabile direttamente nei confronti dei motori di ricerca. Questi sono ritenuti responsabili per la continuata accessibilità di tali notizie, ogni qualvolta la *privacy*, nel corso del tempo, sia divenuta prevalente rispetto libertà di espressione, essendo diminuito l'interesse pubblico alla conoscenza delle stesse notizie.

5. *Google Spain: un conflitto giuridico o politico?*

Il processo davanti alla Corte di Giustizia è stato caratterizzato dalla partecipazione di diversi attori, portatori di diversi valori e interessi, che hanno assunto posizioni contrastanti. L'avvocato generale Jääskinen⁶² aveva proposto una decisione antitetica rispetto a quella adottata dalla Corte: egli non solo aveva escluso che Google potesse essere responsabile, ma aveva considerato la stessa immune rispetto a ordini di rimozione, quando si fosse limitata a svolgere la propria fisiologica funzione di

dynamics of privacy and publicity, in L.Floridi (editor), *The protection of information and the right to privacy* (2014), Springer.

⁶¹ Sulle modifiche proposte dal Parlamento, v. C.KUNER et al. (2014), *The proposed ecc.* op. cit.

⁶² Conclusioni dell'Avvocato Generale Niilo Jääskinen., presentate il 25 giugno 2013 (1), nella Causa C-131/12 Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.

indicizzare tutti i contenuti in rete, non essendo, in tale ruolo, titolare di un'elaborazione di dati personali. Inoltre, la preminenza della libertà di espressione, secondo la tradizione nordeuropea, più vicina in questo riguardo all'esperienza statunitense, conduceva Jääskinen a ritenere che la responsabilizzazione del motore di ricerca avrebbe indotto lo stesso alla rimozione dei link a ogni materiale contestato, e che ciò avrebbe comportato un inammissibile pregiudizio alla libertà di espressione-comunicazione di chi avesse pubblicato un'informazione on-line. Anche i pareri degli Stati membri divergevano su importanti questioni. I governi spagnolo, italiano e polacco, nonché la Commissione, ritenevano che «l'autorità nazionale possa ordinare direttamente al gestore di un motore di ricerca di rimuovere dai propri indici e dalla propria memoria intermedia informazioni contenenti dati personali pubblicati da terzi, senza doversi rivolgere previamente o simultaneamente all'editore della pagina web nella quale compaiono tali informazioni». Invece il governo polacco escludeva la legittimità della rimozione dagli indici di un motore di ricerca di informazioni lecitamente pubblicate su Internet⁶³.

I governi greco, austriaco e polacco, nonché la Commissione affermavano che si potesse dar luogo alla rimozione di dati dagli indici solo nelle ristrette condizioni previste per l'opposizione al trattamento, di cui all'art. 14 della direttiva, cioè in presenza di motivi preminenti e legittimi attinenti alla situazione particolare degli interessati, e «non per il semplice fatto che tali persone ritengano che tale trattamento possa arrecare loro pregiudizio o che esse desiderino che i dati costituenti l'oggetto di detto trattamento cadano nell'oblio⁶⁴». Inoltre i governi greco e austriaco reputavano «che la persona interessata debba rivolgersi all'editore del sito web in questione», anziché al motore di ricerca⁶⁵.

Più ampia possibilità di rimozione, ma sempre condizionata a un pregiudizio dell'interessato, a norma dell'art. 7 (f) della direttiva, era affermata invece dai governi spagnolo e italiano⁶⁶. Secondo la Commissione e i governi spagnolo ed italiano, il fatto che l'informazione sia stata pubblicata regolarmente e continui a essere disponibile nella pagina web del titolare iniziale del trattamento non esclude gli obblighi del motore di ricerca. Il governo della Polonia aveva sostenuto, al contrario, che la liceità della

⁶³ Corte di Giustizia, Sentenza della Corte (Grande Sezione) del 13 maggio 2014), nella Causa C-131/12, § 65.

⁶⁴ Ivi, § 90.

⁶⁵ Ivi, § 90.

⁶⁶ Ivi, § 91.

pubblicazione on line escluderebbe l'obbligo di rimozione⁶⁷. La Corte è andata al di là delle opinioni di tutti i governi intervenuti nel processo. Essa ha affermato, accogliendo la tesi dei governi italiano e spagnolo, che «il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita⁶⁸». Secondo la Corte, inoltre, la richiesta di rimozione da parte dell'interessato può essere rivolta direttamente al motore di ricerca, senza l'intervento di un'autorità giudiziaria o amministrativa e senza richiedere la prova di un pregiudizio effettivo all'interessato. Mentre i governi italiano e spagnolo ritenevano possibile «bloccare l'indicizzazione dei dati nella misura in cui arrecasse un pregiudizio all'interessato⁶⁹», la Corte affermava che il diritto all'oblio non presuppone un pregiudizio. La persona interessata ha il diritto incondizionato di ottenere la rimozione delle informazioni collegate al suo nome, diritto che prevale «non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse [del ...] pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona». La prevalenza presuntiva della *privacy* viene meno solo «qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi». La decisione della Corte si basa quindi sugli assunti della lesività dell'aumento di accessibilità fornito dall'indicizzazione, della prevalenza almeno presuntiva dell'interesse alla *privacy* rispetto alla libertà d'informazione, anche rispetto a informazioni legittimamente pubblicate, e dell'irrelevanza del ruolo neutrale degli intermediari rispetto alla responsabilità per violazioni della protezione dei dati. La decisione del caso Google-Spain ha suscitato forti reazioni da parte degli operatori di Internet. Google pur criticando la decisione della Corte, ha iniziato a dar seguito a essa, offrendo un'interfaccia web nella quale gli interessati possano esprimere le proprie doglianze, e procedendo a rimuovere i link contestati, molti dei quali riguardano informazioni di apparente interesse

⁶⁷ Ivi, § 65.

⁶⁸ Ivi., § 88.

⁶⁹ Si utilizza 'interessato' qui nel senso del Codice *Privacy* Italiano.

pubblico. Questo esito censorio è stato interpretato da alcuni come una conferma dell'assurdità della decisione da Corte, che obbliga i provider a esercitare un ruolo improprio, e da altri invece come cinica scelta tattica di Google, che rifiuta di essere selettiva nelle proprie scelte di rimozione, al fine di screditare la decisione dei giudici e ridurre i propri costi⁷⁰. Non si vede peraltro perché Google dovrebbe procedere a rimozioni più selettive, sottoponendosi al rischio di possibili sanzioni nel caso che le proprie valutazioni non dovessero coincidere con l'eventuale successiva decisione autoritativa⁷¹.

Sul tema è intervenuto recentemente Jimmy Wales, il fondatore di Wikipedia, il quale ha qualificato l'esercizio del diritto a essere dimenticato come «profondamente immorale», poiché «la storia è un diritto umano e una delle peggiori cose che una persona possa fare è cercare di tacitare un altro⁷²». Secondo Lila Tretikov, direttore esecutivo della Wikimedia Foundation (l'ente che gestisce Wikipedia) «la Corte europea ha abbandonato la sua responsabilità di difendere uno dei diritti più importanti e universali, il diritto di cercare, ricevere e trasmettere informazione», e di conseguenza «risultati di ricerche accurate stanno sparando in Europa senza spiegazione pubblica, senza prova reale e senza esame giudiziale, di modo che ne risulta un'Internet crivellata di buchi di memoria alla Orwell⁷³». Sembra indubbio che questa decisione contribuirà ad accrescere il divario tra Europa e Stati Uniti in materia di protezione dei dati. Infatti, la costruzione della Corte sembra del tutto incompatibile con alcuni principi fondamentali dell'ordinamento giuridico statunitense. Essa è in evidente conflitto con la libertà di parola garantita dalla costituzione statunitense: non solo la Corte afferma che la *privacy* può limitare la libertà di espressione, ma attribuisce alla prima un ruolo almeno presuntivamente prevalente sulla seconda. Inoltre la tesi della Corte appare incompatibile con l'idea dell'immunità del provider rispetto alle informazioni prodotte da terzi, immunità conferita dal Communication Decency Act (CDA) statunitense e interpretata in modo assai esteso dai giudici americani.

⁷⁰ Notizia riportata in J.OWEN, *Right to be forgotten: Google accused of deliberately misinterpreting court decision to stoke public anger* (2014), The Independent, 3 giugno.

⁷¹ Come si è osservato, l'anelito all'oblio prevale (quasi) sempre e impone al gestore del motore di ricerca, se allertato, di intervenire per correggere il proprio sistema di indicizzazione, v. A.PALMIERI e R.PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google* (2014), *Nuovi Quaderni del Foro italiano*, Quaderno n. 1 (27 maggio 2014), p. 7.

⁷² S.CURTIS e A.PHILIPSON, *Wikipedia founder: EU's right to be forgotten is 'deeply immoral'* (2014), The Independent, (13 agosto).

⁷³ S.CURTIS e A.PHILIPSON (2014), *Wikipedia founder ecc. op. cit.*

Nella decisione della Corte manca anzi ogni riferimento alle limitazioni della responsabilità del provider stabilite dalla Direttiva sul commercio elettronico, benché tali limitazioni siano state ribadite, anche rispetto alla violazione delle norme sulla *privacy*, nell'Articolo 2, comma 3 della proposta di Regolamento Generale sulla Protezione dei dati⁷⁴. Sembra quindi inevitabile che la scelta della Corte favorirà alla divisione di Internet secondo linee nazionali (o regionali), accrescendo la 'balcanizzazione' della rete già in atto rispetto ai paesi che adottano forme più o meno intense di censura: i link a dati da dimenticare saranno inaccessibili agli utenti europei, rimanendo invece a disposizione degli statunitensi. Il Sudamerica, come osservavamo, sembra poter adottare una posizione intermedia tra Stati Uniti ed Europa almeno nel caso brasiliano: pur non escludendo la soggezione dei provider agli ordini autoritativi di rimozione motivati dal diritto all'oblio, la limitazione della responsabilità degli intermediari sembra escludere che questi possano essere soggetti a sanzione per aver respinto richieste private di rimozione, tranne nell'ipotesi di immagini, video o altri materiali contenenti nudità o atti sessuali di carattere privato.

6. Conclusioni

Come si è illustrato nelle pagine precedenti, nella disciplina della protezione dei dati, e in particolare nella regolazione del diritto a essere dimenticati (la rimozione e dell'occultamento, totale o parziale, di informazioni personali da Internet), si contrappongono diversi valori, che hanno diversa importanza in diversi ordinamenti. In particolare, alla preminenza assoluta della libertà di espressione nel sistema giuridico statunitense si contrappone il rilievo della protezione dei dati in Europa, rilievo che è divenuto preminenza presuntiva nella decisione Google-Spain. Alla fiducia nella libertà economica e nel progresso tecnologico tipiche della cultura statunitense si oppongono i più sospettosi atteggiamenti degli europei. Inoltre, negli Stati Uniti l'atteggiamento negativo rispetto alle intromissioni pubbliche nella vita privata dei cittadini è spesso superato di fronte alle pretese esigenze della sicurezza interna e internazionale, mentre gli europei, pur più propensi ad accettare i limiti posti dall'interesse pub-

⁷⁴ Secondo il quale il regolamento si applicherà «without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive».

blico alle proprie attività, sono meno sensibili rispetto alle minacce alla sicurezza. Questi diversi atteggiamenti si traducono in diverse valutazioni giuridiche: ciò che agli uni appare garanzia della dignità e personalità dell'interessato appare agli altri un'inaccettabile limitazione della sfera di libertà dell'individuo.

Ai diversi valori giuridici si affiancano diversi interessi di soggetti pubblici e privati. Innanzitutto l'interesse degli utenti dei motori ad avere accesso alla massima quantità di informazione e a ottenere risposte affidabili, nel senso di risposte che riflettano lo stato delle informazioni disponibili in rete. A questo interesse si unisce l'interesse di chi carica informazioni in rete, e in particolare di chi è l'autore di tali informazioni, a raggiungere la sfera più ampia possibile di lettori e l'interesse delle imprese di Internet a offrire la massima quantità di informazioni ai propri utenti, e a evitare i costi e i rischi connessi all'esercizio di una funzione censoria. A tali interessi si oppone l'interesse dell'individuo a rimuovere informazioni personali pregiudizievoli o comunque sgradite. Gli Stati Uniti sono interessati a mantenere la superiorità delle proprie imprese mentre gli europei sono interessati a limitare tale superiorità e a promuovere le attività delle proprie. In particolare, gli europei non desiderano che i vincoli che essi pongono alle proprie imprese si traducano in una limitata competitività delle stesse rispetto alle imprese statunitensi, esonerate da tali vincoli.

Gli Stati Uniti desiderano conservare la propria preminente influenza sulla governance di Internet, per sostenere a livello globale i propri valori (libertà di espressione, libertà economiche, ecc.) ma anche per tutelare i propri interessi economici e politici. L'Unione europea è interessata a esercitare una maggiore influenza su Internet, per i medesimi scopi, ma con riferimento a valori (*privacy*, dignità, diversità culturale) e interessi parzialmente diversi. Lo stesso può dirsi per i governi di altri paesi, in particolare nel Sudamerica.

La sentenza della Corte si presta a essere interpretata come una decisa affermazione della prospettiva europea, in aperto contrasto con quella statunitense. Ciò può contribuire a rendere tale decisione accettabile e anzi gradita ai cittadini e ai soggetti politici europei, anche a causa della diffusa irritazione nei confronti degli Stati Uniti e delle imprese di Internet, accresciutasi dopo le rivelazioni di Snowden. Alcune pratiche dei principali fornitori di servizi di Internet nella gestione dei dati degli utenti europei (la profilazione degli utenti, l'estesa conservazione dei loro dati, la combinazione di dati concernenti diversi servizi, la commercializzazione di tali dati, ecc) hanno infatti contribuito a generare un sentimento nega-

tivo, la cosiddetta «Googlephobia». Tale sentimento è stato rafforzato dal comportamento fiscale degli stessi fornitori, consistente nell'adozione di strategie tese a minimizzare l'imposizione, trasferendo i profitti negli stati che, all'interno o all'esterno dell'Unione europea, offrissero condizioni più favorevoli.

Infine, il caso Snowden ha da ulteriormente rafforzato quest'attitudine, dandole una connotazione politica, oltre che economica.

È impossibile specificare con precisione il ruolo che i sentimenti appena descritti possono aver giocato nella decisione della Corte. Certamente essi non sono direttamente rilevanti per la giustificazione giuridica di tale decisione, restando estranei alle sue motivazioni giuridiche. Tuttavia, quei sentimenti possono aver contribuito a determinarla, dandole legittimità 'politica' quale scelta a favore dei valori e dei cittadini europei contro il superpotere economico degli operatori statunitensi di Internet e il superpotere politico del loro governo. Resta da vedere se questo sentimento rimarrà saldo di fronte alle implicazioni operative della decisione della Corte. L'accresciuta tutela dell'autodeterminazione sulle proprie informazioni giustificherà davvero, per i cittadini dell'Unione, la compressione della loro libertà d'informazione? Saranno molte le informazioni d'interesse pubblico a essere rese inaccessibili in seguito alle richieste di rimozione e come inciderà tale censura sul dibattito pubblico? E gli obblighi nascenti dal diritto a essere dimenticati (in particolare, l'onere di valutare correttamente caso per caso ogni richiesta di rimozione) pregiudicheranno la capacità competitiva delle imprese europee rispetto alle grandi concorrenti statunitensi, che meglio possono adempiere a tali obblighi, grazie alle superiori risorse economiche e organizzative? I cittadini europei preferiranno accedere ai servizi di Internet offerti ai cittadini statunitensi piuttosto che a quelli europei, per aver accesso a informazioni più complete, usando le tecniche oggi adottate nei paesi governati da regimi repressivi, ad esempio, accedendo a Internet mediante una rete virtuale privata (Virtual Private Network-VPN statunitense)? Solo il tempo potrà dare una risposta ai molti interrogativi sollevati dalla sentenza della Corte Europea, anche alla luce delle reazioni dei sistemi giuridici degli Stati membri a questa decisione innovativa, che pur basandosi su aspetti comuni alle tradizioni europee (*privacy* come aspetto della dignità e diritto all'oblio), trae da essi implicazioni non pienamente condivise neppure in Europa, oltre che avversate di là dall'Atlantico.

Abstract

The paper aims at comparing the perspectives of EU law and US law on data protection and providers' liability, in particular with regard to the Google-Spain case. First we examine the foundational differences between the approaches adopted in the EU and US, with some references also to South American legal systems. Then we examine some significant divergences or convergences between EU and US, such as in particular those emerging with regard to the transmission in the US of passengers name records (PNR) and SWIFT data, the Snowden case, the debate on the new European data protection regulation. Finally, we consider how political attitudes might have influenced the Google-Spain decisions, or in any case, the way in which it has been received in Europe.

Alessandro Mantelero

Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy

SOMMARIO: 1. Premessa - 2. La decisione 'politica' della Corte - 3. La politica 'reattiva' di Google - 4. Una proposta *de jure condendo* - 5. Conclusioni: oltre il caso Google

1. Premessa

La recente decisione della Corte di Giustizia dell'Unione Europea sul caso Google Spain ha dato luogo a molteplici letture focalizzate sul contenuto della decisione e sulla correttezza degli assunti cui sono addivenuti i giudici. Sono state valutazioni talune di apprezzamento, altre di critica; letture purtroppo talora influenzate da una certa carenza di terzietà di un'accademia sempre più adusa ad aver rapporti commerciali con le grandi *corporations*.

Non è dunque intenzione del presente scritto aggiungere un ulteriore commento tecnico alla decisione, già oggetto di altri contributi anche in questo stesso fascicolo. L'indubbia opportuna disamina dei profili tecnico-giuridici ha tuttavia messo in ombra la dimensione 'politica' della decisione e delle reazioni che ne sono conseguite, intendendo con tale aggettivo far riferimento a quegli aspetti ultimi di ogni pronuncia che spesso vengono offuscati dai tecnicismi, ma che invero ne rappresentano la reale ragion d'essere. Come infatti osservato da tempo dalla dottrina, le sentenze, specie quelle delle corti di grado più elevato, hanno un impatto tale sul contesto sociale ed economico che non possono non prendere in considerazione detto contesto ai fini della decisione, seppur facendo questo in maniera non apertamente manifesta. Così pare scontato che, chiamata a pronunciarsi su temi cruciali della moderna società digitale, quali l'efficacia territoriale delle norme in materia di tutela dei dati personali, il ruolo rivestito dai motori di ricerca nel trattamento delle informazioni ed il difficile rapporto fra accesso alle informazioni ed oblio nel contesto digitale, una corte di massimo grado dell'Unione Europea non possa non

assumere *in primis* una decisione di politica del diritto. E così è stato, come indirettamente dimostrato dallo stesso stile argomentativo della sentenza che, specie per quanto concerne il diritto all'oblio, mostra in taluni punti carenze che svelano la chiara intenzione politica della pronuncia. A tal riguardo, due sono gli aspetti che paiono maggiormente rilevanti e fanno della sentenza un elemento significativo nella costruzione del diritto comunitario dell'informazione: l'applicabilità del diritto comunitario a chi offre servizi ai cittadini dell'Unione, il sostanziale supporto al riconoscimento del diritto alla cancellazione dei dati personali. Entrambi questi profili costituiscono nel contempo punti centrali e rilevanti della proposta di regolamento comunitario in materia di tutela dei dati personali ormai entrata nella fase finale del proprio *iter*¹. Profili inoltre controversi per via delle chiare implicazioni e ricadute sui modelli di *business* adottati da alcuni dei maggiori operatori del mercato digitale. In proposito la decisione pare dunque 'anticipare' alcune previsioni del nuovo quadro normativo che si sta delineando². Nel far questo, tuttavia, i giudici hanno operato sulla base dell'esistente contesto regolamentare incentrato sull'ormai datata dir. 95/46/CE; non stupisce dunque che le argomentazioni risultino talora deboli in termini di ricadute pratiche ed operative. Ricadute operative che rivestono un elemento cruciale nel contesto dell'economia digitale, lad-

¹ Cfr. Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25/01/2012, in http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf; Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 - C7 0025/2012 - 2012/0011(COD)), compromise amendments on Articles 1-29 and on Articles 30-91, in http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_01-29/comp_am_art_01-29en.pdf e http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/comp_am_art_30-91/comp_am_art_30-91en.pdf. Nel marzo 2014, il testo adottato dalla Commissione Libertà civili, giustizia e affari interni è stato approvato dal Parlamento Europeo, cfr. <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN>. Cfr. anche A. MANTELERO, *La riforma della data protection in Europa: un'opportunità per le imprese*, in giustiziacivile.com, 3 marzo 2014, in <http://giustiziacivile.com/soggetti-e-nuove-tecnologie/approfondimenti/la-riforma-della-data-protection-europa-un-opportunit-le>. Tutti i link ipertestuali cui è fatto rinvio nelle presenti note sono riferiti a contenuti disponibili *online* e visionati nel periodo compreso fra il 20/05 ed il 16/07/2014.

² In senso critico rispetto alle conclusioni cui è addivenuta la Corte, cfr. A. PALMIERI, R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quaderni del Foro italiano*, Quaderno n. 1, 2014.

dove occorre trovare il giusto bilanciamento fra tutela dei diritti ed incrementi degli oneri per le imprese. Pare tuttavia opportuno ribadire come la libertà di impresa, ancorché riconosciuta nelle carte fondamentali, rimane pur sempre subordinata alla protezione degli interessi della persona come singolo e come parte delle comunità sociali. Con buona pace degli operatori economici, sono dunque i modelli di *business* a doversi adeguare al rispetto dei diritti fondamentali e non viceversa. In tal contesto va dunque apprezzata la presente decisione, la cui finalità non pare tanto quella di definire una disciplina destinata ad essere transitoria, stante l'imminente riforma, quanto piuttosto proprio a supportare le linee di intervento di tale nuova definizione del quadro normativo, con riguardo ad uno dei punti oggetto di maggiori critiche. È infatti a tutti noto come proprio sull'art. 17 della proposta di regolamento comunitario in materia di tutela dei dati personali, inerente il diritto alla cancellazione (originariamente rubricato come «right to be forgotten»), si siano concentrate le critiche di molti e le lobbies abbiano esercitato una forte azione di contrasto³. Le regole operative che derivano dalla sentenza sono in parte incerte e non del tutto definite, ma dando una lettura appunto politica della decisione si potrebbe ritenere che proprio questo effetto sia stato voluto. L'incertezza derivante dal quadro esistente e la concomitante decisa affermazione del diritto alla cancellazione, dovrebbero infatti indurre a riflettere sull'op-

³ Cfr. a riguardo AMERICAN CHAMBER OF COMMERCE TO THE EUROPEAN UNION, *AmCham EU Proposed Amendments on the General Data Protection Regulation*, s.d., 22 ss., consultabile online all'indirizzo http://www.laquadrature.net/wiki/images/0/00/AmCham_EU_Proposed_Amendments_on-Data_Protection.pdf [consultato il 30/09/2014]; Facebook recommendations on the Internal Market and Consumer Affairs draft opinion on the European Commission's proposal for a General Data Protection Regulation «on the protection of individuals with regard to the processing of personal data and on the free movement of such data», s.d., 30 ss. Consultabile online all'indirizzo http://www.laquadrature.net/wiki/images/3/3b/20121026_Drafting-recommendations_IMCO-draftopinion_final.pdf [consultato il 30/09/2014]. I due documenti citati fanno parte di una più ampia rassegna dei documenti predisposti dai diversi gruppi di lobbying la cui raccolta è stata realizzata da La Quadrature du Net, consultabile online all'indirizzo http://www.laquadrature.net/wiki/Lobbies_on_dataprotection#AmCham.2C_January_2013 [consultato il 30/09/2014]; cfr. anche C. ARTHUR, *UK joins USin lobbying Brussels over data protection rules*, in *The Guardian*, 7 marzo 2013, consultabile online all'indirizzo <http://www.theguardian.com/technology/2013/mar/07/uk-us-eu-data-protection-rules> [consultato il 30/09/2014]; N. LOMAS, *Facebook Lobbying Europe On «Unreasonable And Unrealistic» Privacy Law Reform - But EC Commissioner Doesn't Sound Like She's For Turning*, in *TechCrunch*, 9 novembre 2012, consultabile online all'indirizzo <http://techcrunch.com/2012/11/09/facebook-lobbying-europe-on-unreasonableand-unrealistic-privacy-law-reform-but-eccommissioner-doesnt-sound-like-shes-forturning/> [consultato il 30/09/2014].

portunità di non depotenziare, bensì migliorare l'art. 17 della proposta, attraverso una più chiara definizione delle modalità operative dello stesso.

A parere di chi scrive, questo è stato il messaggio affidato dalla Corte ai decisori ed alle parti interessate. In tale ottica nelle pagine che seguono verranno prese in esame sia le finalità della decisione, sia la reazione di Google. Anche rispetto a quest'ultimo profilo, le reali intenzioni paiono infatti andare al di là della formale adesione al verdetto e mirare a generare un dibattito sulle scelte di politica del diritto da adottarsi in materia. Da qui la necessità di delineare soluzioni adeguate che si collochino nel contesto della più ampia evoluzione della regolamentazione in tema di trattamento delle informazioni cui si sta assistendo a livello globale.

In tale percorso quello che pare talvolta mancare è la maturità del mondo imprenditoriale nel comprendere come politiche orientate alla tutela dei diritti degli utilizzatori dei servizi e, più in generale, dei cittadini possano avere ricadute favorevoli in un'ottica competitiva, più di quanto non accada con politiche di tipo 'aggressivo', volte a massimizzare gli interessi commerciali⁴.

2. La decisione 'politica' della Corte

Quando le corti supreme assumono provvedimenti destinati ad incidere direttamente sulle strategie di grandi operatori economici, nonché sulle dinamiche dei mercati in cui questi sono attivi, è inevitabile che tanto le logiche seguite dagli autori della pronuncia quanto quelle dei destinatari della stessa trascendano, almeno in parte, dalla mera applicazione delle regole giuridiche. In tal senso, gli annali di giurisprudenza, e quelli delle corti supreme in specie, sono ricchi di sentenze in cui l'obiettivo primario è di politica del diritto e le motivazioni giuridiche risultano funzionali. Queste pronunce — tra cui va annoverata quella in esame — mancano talora di linearità e completezza⁵, tuttavia assolvono al fine di affermare la tutela di uno specifico aspetto, dando risposta a precise istanze sociali.

⁴ Cfr. a riguardo le osservazioni espresse in A. MANTELERO, *Competitive value of data protection: the impact of data protection regulation on online behavior*, in *International Data Privacy Law*, (2013) pp. 3 (4): 229-238, in <http://idpl.oxfordjournals.org/content/3/4/229> [consultato il 30/09/2014].

⁵ Cfr. a titolo d'esempio Cass., 20 aprile 1963, n. 990, in *Giust. civ.*, 1963, I, pp. 1280 ss. (in materia diritto alla riservatezza); Cass., S.U., 11 gennaio 2008, n. 576, in *Le banche dati de Il Foro it.* (in materia di danni da emoderivati).

Istanze sovente confliggenti con paradigmi tradizionali, le quali necessitano di risposte nuove volte a rimodellare il sistema alla luce delle emergenti esigenze di tutela. Rileggendo in quest'ottica la pronuncia della Corte di Giustizia, il baricentro dell'attenzione si sposta dunque dalla correttezza formale del ragionamento alla *ratio* 'politica' della decisione, tesa quale logica ispiratrice dell'agire dei giudici nella prospettiva dell'incidenza della pronuncia sul contesto sociale latamente inteso.

La corte avrebbe potuto seguire la linea tracciata dall'Avvocato Generale, che in ultima analisi avrebbe consentito di conservare lo *status quo*. Questo avrebbe preservato le prassi esistenti affermatesi nelle giurisprudenze delle autorità garanti in materia di bilanciamento fra diritto di informazione e diritto all'oblio. Prassi che hanno visto come destinatari non i motori di ricerca, bensì i siti sui quali erano pubblicate le informazioni oggetto di contestazione, richiedendo a quest'ultimi di rendere non indicizzabili i contenuti in questione⁶ ed addivenendo in tal modo ad un bilanciamento fra il legittimo diritto all'oblio ed il diritto di essere informati⁷.

La corte ha invece riconosciuto il diritto del singolo a non vedere indicizzati fra i risultati della ricerca le informazioni personali che risultino «inadequate, irrelevant or no longer relevant, or excessive» rispetto alle finalità del trattamento. I giudici, correttamente, non hanno dunque confuso il diritto alla cancellazione con il diritto all'oblio ed in tal senso la pronuncia è più orientata ad un (implicito) confronto con l'art. 17 della proposta di regolamento comunitario in materia di tutela dei dati personali, piuttosto che con la sola giurisprudenza in materia di diritto all'oblio⁸.

⁶ Cfr. Opinion of Advocate General Jääskinen, delivered on 25 June 2013, Case C 131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, §§ 41-42, in Appendice a questo Volume. Cfr. anche Gar., 11 dicembre 2008 [doc. web n. 1583162].

⁷ Cfr. A. MANTELERO, Right to be forgotten *ed archivi storici dei giornali*. La Cassazione travisa il diritto all'oblio, in *Nuova giuri. civ. comm.*, 2012, pp. 543-549.

⁸ Con riguardo al riconoscimento del diritto all'oblio nell'ordinamento statunitense ed in Europa, cfr. P. BERNAL, *The EU, the US and Right to be Forgotten*, in S. GUTWIRTH, R. LEENES, P. DE HERT (eds), *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenge*, Springer, 2014, 61 ss.; S.C. BENNETT, *The «Right to Be Forgotten»: Reconciling EU and US Perspectives*, 30 *Berkeley J. Int'l Law* 161 (2012); F. WERRO, *The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash*, in A. COLOMBI CIACCHI, C. GODT, P. ROTT, L.J. SMITH (eds), *Haftungsrecht im dritten millennium*, Nomos, 2009, 285 ss. Cfr. anche P. M. SCHWARTZ, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 *Harv. Law Rev.* 1966, 1994-1995 (2013). Per un raffronto anche con il disposto dell'art. 17 proposta di regolamento comunitario in materia di tutela dei dati personali, si veda anche, volendo, A. MANTELERO, *The EU Proposal for a General*

Tale distinguo è invece talora sfuggito ai commentatori della pronuncia, in ciò indotti dalla fattispecie concreta che ha dato adito alla decisione.

Un altro equivoco ricorrente nei commenti alla pronuncia è la confusione fra possibilità di rintracciare un'informazione disponibile *online* avvalendosi di un motore di ricerca e diritto ad essere informati. Occorre in proposito distinguere il bilanciamento fra diritto all'informazione e diritto all'oblio, i cui criteri sono stati da tempo definiti dalla giurisprudenza, dal diverso profilo inerente il riconoscimento del diritto alla cancellazione ai dati trattati esercitato al di fuori del contesto dei *media*. Sul punto va osservato come la pronuncia avrebbe potuto argomentare con maggior chiarezza, sebbene tale distinzione paia comunque emergere nelle motivazioni⁹.

In sintesi dunque la pronuncia risulta in linea con il dettato della direttiva¹⁰ e, alla luce del vigente quadro normativo, non pare esservi nulla di controverso nel fatto che l'interessato possa rivolgersi al gestore del motore di ricerca per chiedere la rimozione dei contenuti ritenuti non coerenti con le finalità del trattamento. Tuttavia proprio su questo punto emerge l'inevitabile tensione che caratterizza la fattispecie e, conseguentemente, emerge la valenza politica della pronuncia.

Se è infatti vero che Google per prima rigetta l'equiparazione con i *media*, in ragione degli evidenti benefici in termini di esonero dal controllo sui contenuti, purtuttavia da un punto di vista della comunicazione è evidente come la convergenza in atto fra i diversi *media* ed il ruolo assunto da Internet nella società, rendono di fatto i motori di ricerca la porta di accesso ed il filtro ai contenuti disponibili in Rete. In tal contesto, riconoscere il diritto al singolo alla cancellazione dei dati ed individuare — correttamente, stante la normativa vigente — nel gestore del motore di

Data Protection Regulation and the roots of the 'right to be forgotten', in *Computer Law and Security Review*, (29) 2013, pp. 229-235, <http://dx.doi.org/10.1016/j.clsr.2013.03.010> [consultato il 30/09/2014] («The different representation of the right to be forgotten as the right to have personal data completely removed is consistent with the notion of droit à l'oubli, but in this case it has a wider scope, because the erasure of the data is not only related to the loss of interest in past events, but also to other situations (e.g. wrongful or illicit data processing) that do not concern the balance between media and individual life”).

⁹ Cfr. Corte Giustizia UE, 13 maggio 2014, C 131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, pp. 92-99, in Appendice a questo Volume.

¹⁰ Cfr. Article 29 Data Protection Working Party, Press Release, Brussels, 23/05/2014, in http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140523_wp29_press_release_ecj_google.pdf [consultato il 30/09/2014].

ricerca il destinatario dell'istanza, nonché il soggetto deputato a valutarne l'accoglimento, crea un'inevitabile frizione. L'esercizio dei diritti dell'interessato (i.e. cancellazione dei dati, rettifica aggiornamento ecc.), non controverso quando posto in essere nei confronti di un qualunque titolare del trattamento, assume connotati ben differenti laddove affermato nei confronti di uno dei pochi *gatekeepers* della conoscenza *online*. In questo caso infatti la decisione circa la rimozione del contenuto figurante nei risultati della ricerca ha un immediato effetto di nascondimento rispetto all'informazione ospitata sul sito web cui il link indicizzato puntava. Quest'ultima informazione continuerà infatti ad esistere nella sua collocazione originaria, ma nei fatti non sarà pressoché raggiungibile dalla maggior parte degli utenti. In virtù delle modalità proprie dell'organizzazione e gestione dei contenuti disponibili *online*, il diritto alla cancellazione si traduce quindi in una sorta di diritto alla non reperibilità *de facto* del dato, o almeno alla sua limitata e circoscritta fruibilità. Ne consegue che, non sotto il profilo eminentemente giuridico inerente il trattamento dati, bensì sul piano operativo, la decisione incide sul diritto all'informazione, nella sua duplice natura di diritto ad informare e ad essere informati.

Emerge così l'*impasse* intrinseco alla pronuncia, che da un lato deve necessariamente rendere il titolare del trattamento decisore in conformità al dettato della disciplina in materia di *data protection*, ma nel contempo così facendo, lo tramuta in un arbitro della fruibilità dell'informazione *online*, in ragione della natura del soggetto in questione (motore di ricerca).

In questo caso si palesano dunque i limiti di una regolamentazione (quella definita con la direttiva) ormai vecchia di vent'anni e, per questo, non sempre in grado di fornire risposte efficaci al mutato contesto tecnologico e sociale. Trattare Google o qualsiasi altro motore di ricerca alla stregua di un qualunque titolare di una raccolta di dati personali è infatti inadeguato. La valutazione che qui occorre circa la validità delle pretese dell'interessato è infatti ben più complessa di quanto non accada in un'ordinaria richiesta di cancellazione di un dato obsoleto o incoerente con le finalità della raccolta. In particolare, a causa delle conseguenze in termini di diritto ad essere informati, è foriera di implicazioni ben più ampie, che potenzialmente interessano la collettività. Per questa ragione pare possibile ravvisare una linea di politica del diritto nella posizione assunta dalla Corte che, rifiutando quella che poteva essere l'*exit strategy* basata sulle argomentazioni dell'Avvocato Generale, ha finito per porre l'attenzione sui limiti attuativi dei principi affermati dal modello in essere, inducendo

così la riapertura del dibattito sull'assai controverso articolo 17 della proposta di regolamento comunitario in materia di tutela dei dati personali.

A ridosso delle fasi finali dell'approvazione del nuovo regolamento, l'aspettativa di vita della pronuncia pare infatti essere assai breve, ma le criticità operative che ne scaturiscono costituiscono un valido incentivo ad introdurre adeguate soluzioni nella normativa *in fieri*. Se, a tal riguardo, si tiene in conto dell' incisiva attività di *lobbying* ai danni del testo originario dell'art. 17¹¹, trova ulteriore conferma la valenza orientativa e 'politica' della decisione in esame.

I limiti connaturati al *decisum* sono infatti tali da dover necessariamente indurre ad una soluzione più efficiente del problema, soluzione che proprio l'art. 17 potrebbe offrire. Tralasciando le riflessioni circa l'inopportunità delle modifiche apportate al testo originario dell'articolo 17 (nonché la valutazione delle soluzioni alternative che si sarebbero potute adottare), merita tuttavia osservare come il testo attualmente in discussione contempli esplicitamente la cancellazione dei dati allorquando «a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased». In questo la pronuncia della Corte può dunque essere letta come un indiretto supporto alla soluzione indicata dalla riforma: demandare ad un'autorità giudiziaria o alle autorità garanti per la protezione dei dati il compito di effettuare quel bilanciamento fra interessi individuali e collettivi che è bene che non venga demandato ad un soggetto privato dominante quale Google¹². Al riguardo un'efficace regolamentazione del diritto alla cancellazione come definito dal menzionato art. 17 potrebbe dunque trovare ora anche il supporto di settori imprenditoriali in precedenza fortemente critici, al fine di evitare lo *status quo* creato dalla sentenza che rischia di far figurare alcune delle maggiori imprese IT come 'censori' della Rete. In conclusione dunque, la lettura della pronuncia che qui si propone è quella che ravvisa nella decisione l'intento di porre in tensione il quadro normativo esistente a beneficio della riforma dello stesso, riforma spesso fortemente osteggiata da parte del mondo imprenditoriale.

3. La politica 'reattiva' di Google

Se la lettura della sentenza è dunque di politica del diritto, va rilevato

¹¹ Cfr. *supra* nota 2.

¹² Cfr. anche Opinion of Advocate General Jääskinen, cit., § 134.

come anche la reazione del destinatario della pronuncia si sia mossa in gran parte sul medesimo piano. Tale reazione induce a riflettere su come il gigantismo dei destinatari delle decisioni, unito alle peculiarità connesse al potere di incidere sulle dinamiche *online*, possa sortire effetti che paiono non aver precedenti. In mancanza di esplicite indicazioni volte a chiarire nello specifico i fini della complessa strategia intrapresa da Google, non è possibile far altro che esprimere un parere puramente scientifico di tipo induttivo. Quella che sembra delinearsi è una strategia di impresa che formalmente adempiendo alla pronuncia ne mina di fatto il fondamento, favorendo in tal maniera le opinioni critiche circa le ragioni e l'attualità del diritto alla cancellazione ed all'oblio nel moderno contesto delle comunicazioni *online*¹³. In primo luogo il gestore del motore di ricerca ha deciso di creare uno spazio online *ad hoc* per consentire a tutti gli utenti di inoltrare una richiesta di cancellazione¹⁴. Trattasi di un adempimento non richiesto dalla Corte, che pare inoltre un *unicum* rispetto alle molte altre tipologie di comportamenti illeciti che possono essere posti *online* e che risultano correlati ai servizi erogati da Google. Non si coglie poi la ragione di tale mutamento delle modalità di gestione delle richieste in questione, posto che da anni Google riceve simili istanze, attraverso le vie ordinarie previste per l'esercizio dei diritti riconosciuti dalle normative locali in attuazione dell'art. 12, Dir. 95/46/CE. È invece del tutto evidente come tale 'servizio', immediatamente pubblicizzato dai media di tutto il mondo, favorisca (anche per le più agevoli modalità) un picco di domande. L'effetto di questo picco è molteplice: dimostra l'onere derivante dalla sentenza in capo al gestore del servizio, paventa eventuali conseguenze rilevanti in termini di cancellazione di informazioni dalla Rete, accresce la funzione valutativa in capo a Google, consente a quest'ultimo un'ampia discrezionalità nella scelta di quali richieste privilegiare.

Il tutto senza che tale inusuale procedimento sia assistito da un adeguato grado di trasparenza che permetta di comprendere esattamente quale tipologia di richieste è stata avanzata e da quali categorie di soggetti esse provengono, onde poter valutare se i primi provvedimenti di rimozione adottati dalla società risultino coerenti con la normalità delle richieste o costituiscano ipotesi del tutto eccentriche rispetto ad essa. Prima di esaminare tali casi di rimozione, va sin da subito sottolineato come siano pro-

¹³ Cfr. J. ROSEN, *The Right to Be Forgotten*, in 64 *Stan. L. Rev. Online* 88, February 13, 2012.

¹⁴ Cfr. il modello di «Richiesta di rimozione di risultati di ricerca ai sensi della legge europea per la protezione dei dati», disponibile al seguente indirizzo: https://support.google.com/legal/contact/lr_eudpa?product=websearch [consultato il 30/09/2014].

prio i limiti dell'esistente dettato normativo a favorire un'ampia discrezionalità di azione in capo ad un soggetto imprenditoriale che detiene il 90% del *market share* europeo nel settore dei motori di ricerca. In quest'ottica, l'analisi dei casi merita indubbia attenzione e può fornire elementi per una possibile lettura della politica adottata dal destinatario della pronuncia in esame. Esempiare pare essere il caso che ha coinvolto un articolo di commento sulla vicenda finanziaria della Merrill Lynch pubblicato sul sito della BBC («Merrill's mess»¹⁵), laddove la richiesta di rimozione (i cui termini non sono noti) proveniva non dal soggetto interessato dalla notizia¹⁶, bensì da una persona che aveva postato un commento all'articolo¹⁷. Nella specie la notorietà della notizia escludeva qualsiasi questione circa il diritto all'oblio rispetto all'attività dei *media* e la richiesta di cancellazione proveniente dal commentatore non poteva certo giustificare la de-indicizzazione del contenuto dell'articolo cui il singolo commento si riferiva. La reazione da parte di Google è dunque apparsa quantomeno contrastante con il principio di proporzionalità che connota, tra le altre, anche la materia della *data protection*.

Non è dato sapere per quale ragione sia stato scelto questo caso, né perché non si siano valutate soluzioni alternative rispetto alla rimozione integrale, compresa quella di trasferire il contenzioso davanti alla *data protection authority* competente. Certo rimane il fatto che la decisione (sproporzionata), cui è seguita la reintegrazione dell'articolo, ha avuto l'effetto di inasprire le critiche indirizzate contro la pronuncia della Corte¹⁸. Nel contempo, il caso indica un ulteriore punto di conflitto, rappresentato dai commenti alle notizie e dalla possibilità, non solo giuridica, ma anche

¹⁵ Cfr. R. PESTON, *Merrill's mess*, in *BBC*, 29 October 2007, in http://www.bbc.co.uk/blogs/legacy/reporters/robertpeston/2007/10/merrills_mess.html [consultato il 30/09/2014].

¹⁶ Trattavasi di Stan O'Neal, chairman di Merrill Lynch all'epoca della notizia.

¹⁷ Questa la ricostruzione dei fatti effettuata dal giornalista autore dell'articolo inizialmente rimosso, cfr. R. PESTON, *Why has Google cast me into oblivion?*, in *BBC News Business*, 02/07/2014, in <http://www.bbc.com/news/business-28130581> [consultato il 30/09/2014].

¹⁸ A riguardo ha influito anche l'ulteriore modalità di attuazione della pronuncia ad opera di Google, consistente nella notifica al gestore del sito dell'avvenuta rimozione. Provvedimento in sé condivisibile, come si avrà modo di affermare nel prosieguo nel testo, ma che ove i destinatari siano alcune delle maggiori testate giornalistiche inglesi, ha l'indubbio effetto di ingenerare una scontata reazione dei media, non certo favorevole alla decisione della Corte. Cfr. R. PESTON, *Why has Google cast me into oblivion?*, cit.; J. BALL, *EU's right to be forgotten: Guardian articles have been hidden by Google*, *The Guardian*, 2 July 2014, in *The Guardian*, in <http://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google> [consultato il 30/09/2014].

tecnica, di esercitare in maniera ‘chirurgica’ il diritto alla cancellazione rispetto a singole opinioni espresse. Un altro dei primi casi di rimozione dei contenuti ha invece riguardato una fattispecie che si colloca pienamente nell’ambito del diritto all’oblio¹⁹, rispetto alla quale è divenuta concretamente evidente quella che pare costituire la maggiore criticità correlata all’applicazione dei principi delineati dalla Corte, inerente il bilanciamento di interessi.

A fronte di una pretesa lesione del diritto all’oblio è infatti possibile addivenire alla rimozione delle informazioni solo a seguito di un preventivo bilanciamento fra gli interessi collettivi alla conoscenza dei fatti e quello individuale alla cancellazione delle informazioni. Bilanciamento che tradizionalmente compete ai *media* i quali, per ruolo professionale e per la conoscenza dei fatti concreti, sono nella posizione migliore per farvi fronte. L’apparire dei nuovi intermediari della comunicazione ha invece creato un ulteriore livello nella circolazione delle informazioni in precedenza sconosciuto. Mentre in passato era il giornalista a fare da intermediario tra i fatti (e la tutela dei diritti di coloro che in essi erano coinvolti) e la collettività, ora invece tale ruolo è in parte esercitato dagli intermediari della Rete. I motori di ricerca (ma la riflessione potrebbe estendersi anche ad altri aggregatori di contenuti) consentono infatti un accesso diffuso alla notizia, favorendone la propalazione, senza però esercitare alcun controllo editoriale sui contenuti, come invece avviene nella mediazione giornalistica. Da qui la tensione emersa nei casi inerenti il diritto all’oblio allorquando l’interessato scelga la via breve consistente nell’agire direttamente contro il gestore del motore di ricerca piuttosto che contro la testata giornalistica. Ove ciò avvenga, la normativa sui dati personali finisce per richiedere al motore di ricerca di porre in essere un bilanciamento di interessi²⁰ che esula dal proprio ruolo e dalle proprie competenze, mancando sia la diretta conoscenza delle vicende sia la specifica professionalità. Questo non implica che il motore di ricerca debba necessariamente essere escluso dal processo di rimozione dei contenuti e che il destinatario della pretesa debba essere solamente il soggetto che ha pubblicato originariamente la notizia. Laddove si verta in materia di libertà di informazione, parrebbe tuttavia utile introdurre opportune disposizioni che prevedano l’attivarsi del motore di ricerca ai fini della rimozione solo a fronte di una valutazione proveniente dall’autorità giudiziario o dall’autorità per la pro-

¹⁹ Cfr. C. DYER, *Accused solicitor stands for office*, in *The Guardian*, Friday 28 June 2002, in *The Guardian*, in <http://www.theguardian.com/uk/2002/jun/28/claredyer> [consultato il 30/09/2014].

²⁰ Cfr. Corte Giustizia UE, 13 maggio 2014, C 131/12, cit., § 81.

tezione dei dati o, quantomeno, in seguito ad istanza del gestore del sito che ospitava i contenuti rimossi²¹.

Del terzo caso oggetto di rimozione²² qui considerato non è dato comprendere le ragioni. Trattasi di un articolo giornalistico in cui compaiono a margine, in chiusura, i nominativi di due intervistati in un contesto affatto pregiudizievole. Non paiono sussistere ragioni in termini di diritto all'oblio, e qualora il fondamento fosse ravvisabile nel diritto alla cancellazione degli intervistati, stante la marginalità delle loro affermazioni, la rimozione dell'intero articolo parrebbe comunque sproporzionata. Anche qui il caso tuttavia suggerisce un aspetto meritevole di attenzione: v'è distinzione fra un articolo *online* che è totalmente incentrato su una vicenda personale, rispetto alla quale è evidente il possibile interesse del singolo alla tutela dell'oblio, dalla diversa situazione in cui le informazioni relative all'interessato abbiano un ruolo assolutamente marginale nel contesto informativo, tanto più se anche prive di carattere pregiudizievole. Se infatti è vero, che proprio il suddetto metodo di ricerca testuale rende ogni parte del testo indicizzabile, tuttavia applicando il principio di proporzionalità nella fattispecie da ultimo esaminata si deve ritenere che il diritto del singolo, sia esso all'oblio o alla cancellazione, non possa pregiudicare l'intera notizia. In ragione di ciò il destinatario più opportuno ai fini dell'esercizio di tale diritto appare il gestore della pagina web che ospita il contenuto piuttosto che il motore di ricerca. Il primo infatti, sempre sulla base di un bilanciamento di interessi, può ventualmente valutare l'opportunità di adottare soluzioni tecniche volte a limitare l'accesso al singolo commento. Il quarto caso consiste infine in una rassegna degli articoli apparsi durante un'intera settimana sul *Guardian* ad opera di uno dei giornalisti della testata²³, anche qui è oscura la ragione di un provvedimento che pare sproporzionato. A valle di queste rimozioni (e successive reintegrazioni) occorre non solo riflettere sulle criticità che le stesse evidenziano, ma anche chiedersi come mai fra decine di migliaia di richieste²⁴ che riguarderebbero «reati

²¹ Cfr. art. 17 (ca), proposta di regolamento comunitario in materia di tutela dei dati personali.

²² Cfr. J. HENLEY, *Paris's Post-it wars*, in *The Guardian*, Tuesday 30 August 2011, in <http://www.theguardian.com/artanddesign/2011/aug/30/paris-post-it-warsfrench> [consultato il 30/09/2014].

²³ La rassegna è reperibile al seguente indirizzo: <http://www.theguardian.com/media/green-slade/2011/oct/31/week> [consultato il 30/09/2014].

²⁴ Cfr. EDITORIAL BOARD, *UnGoogled: The disastrous results of the 'right to be forgotten' ruling*, 12/07/2014, in *The Washington Post*, in http://www.washingtonpost.com/opinions/ungoogled-the-disastrous-results-of-the-right-to-be-forgottenruling/2014/07/12/91663268-07a8-11e4-bbf1-cc51275e7f8f_story.html [consultato il 30/09/2014].

gravi, foto imbarazzanti, episodi di bullismo o di insulti online, vecchie denunce, articoli di giornale screditanti e molto altro»²⁵, provenienti da tutto il mondo, l'attenzione di Google si sia incentrata su casi controversi e coinvolgenti le maggiori testate britanniche. Casi che paiono ben lontani dalla vicenda dell'oscuro avvocato del quotidiano catalano che ha dato vita alla pronuncia della Corte, suscettibili (per oggetto, testata, lingua, etc.) di assai maggior risonanza mediatica. Se dunque sul piano giuridico questi 'casi scelti' mettono in luce alcuni aspetti meritevoli di approfondimento, è pur vero che sul piano mediatico e comunicativo questi provvedimenti hanno indubbiamente sortito l'effetto di far apparire molto controversa la posizione assunta dall'Unione Europea, specie Oltreoceano dove le differenze culturali rendono ancor più difficile cogliere il quadro giuridico comunitario²⁶. Diversa sarebbe stata la percezione se si fosse deciso di rimuovere i contenuti inerenti «reati gravi, foto imbarazzanti, episodi di bullismo o di insulti online», sollevando invece le criticità sopra evidenziate in maniera più formale ed in più opportuni contesti (es. Article 29 Working Party, *data protection authorities*).

Esiste una sottile linea che demarca il confine fra adempiere ad una pronuncia e darvi seguito in una maniera discrezionale tale da esasperarne i limiti. È mancata dunque la definizione di una chiara procedura di rimozione, un coinvolgimento cooperativo dei *media* (ridotti a meri destinatari di notifiche, utili soprattutto ad indurre pubbliche reazioni di sdegno), un dialogo attivo con le autorità di protezione dei dati. La sensazione è invece che nel dar seguito ad una pronuncia non certo gradita, su un tema da tempo oggetto di conflitto, si sia preferito un approccio da «over the top», intento a spostare il discorso dal piano giuridico a quello mediatico e dell'opinione pubblica. In tal senso sembrano deporre non solo le scelte di rimozione di cui si è detto, ma anche altri elementi a partire dal 'referendum' *online* sulla sentenza sino al gruppo di esperti costituito *ad hoc*. Riguardo alla prima iniziativa, trattasi di una pagina web che intende raccogliere le opinioni degli utenti di Internet in risposta al seguente quesito: «Come dovrebbe essere bilanciato il diritto all'oblio di una persona con il diritto del pubblico di sapere?»²⁷. Onde rispondere all'esortazione «Facci sapere che cosa pensi della sentenza della CGUE», all'utente viene fornito un testo descrittivo del problema che risulta privo di alcun rimando alla pronuncia, parte di essa o anche solo al relativo comunicato stampa. La sintesi della *ratio decidendi* è così espressa: «i cittadini europei hanno ora

²⁵ Cfr. <https://www.google.com/advisorycouncil/> [consultato il 30/09/2014].

²⁶ Cfr. J. ROSEN, cit. Cfr. anche *supra* nota 8.

²⁷ Cfr. <https://www.google.com/advisorycouncil/> [consultato da ultimo in data 14/07/2014].

il diritto di richiedere la rimozione dai motori di ricerca, ad esempio da Google, dei risultati relativi a ricerche che includono il loro nome». Si chiedono poi «consigli sui principi che Google dovrebbe applicare per prendere decisioni in merito ai singoli casi [...] ci piacerebbe sapere che cosa pensi di queste tematiche. Dopotutto si tratta dei tuoi diritti online e Internet rappresenta un grande luogo di confronto e discussione». Traspare anche qui un uso peculiare della posizione di strutturale vantaggio di Google, derivante dalla possibilità di interagire quotidianamente e costantemente con milioni di persone, onde raccogliere quella che si vorrebbe rappresentare come la «wisdom of the crowd». Qui tuttavia il tema è giuridico, nonché connotato da significativo tecnicismo. Rispetto ad esso pare dunque difficile attribuire un valore ad una simile pubblica consultazione, se non quello di trasformarla in una sorta di referendum pro o contro la decisione della Corte di Giustizia. Occorre evitare il rischio che i diritti fondamentali ed il loro bilanciamento finiscano per essere tradotti nella forza muscolare del numero di «like». Un eventuale approccio di tipo statistico e sociologico sulla base dei commenti raccolti, che porti a concludere cosa «pensa la Rete» della decisione può forse essere utile in termini di suggerimenti, ma non può in alcun modo costituire una sorta di appello rispetto ad una decisione di una massima autorità giudiziaria. I cittadini che non condividono le idee espresse dalla pronuncia hanno canali istituzionali per far valere le proprie opinioni, a partire dai loro rappresentanti presso l'Unione Europea ove è in discussione il nuovo *framework* comunitario in materia di *data protection*. Vi sono poi le organizzazioni rappresentative degli interessi collettivi e le forme tradizionali della libertà di espressione. Non dunque un sondaggio privo di adeguata informazione e le cui finalità paiono non del tutto nitide. Non priva di criticità è anche la nomina di un gruppo di esperti *ad hoc* da parte di Google, affinché «raccolga le opinioni degli europei e [...] aiuti così a esaminare la questione» ed «al fine di far emergere e approfondire le relazioni complesse che intercorrono tra il diritto di sapere e il diritto alla *privacy*». In *primis* v'è da chiedersi per quale ragione un'impresa chiamata ad adempiere ad una sentenza abbia bisogno di esperti nominati con tanta propaganda, quando dispone di numerosi valenti legali. Così come non è dato comprendere perché privilegiare il dialogo con esperti selezionati dalla stessa impresa anziché quello con le autorità istituzionalmente deputate ad occuparsi di *data protection*. Nuovamente si ha la sensazione di un approccio da «over the top».

Trattasi di un comitato che opererà anche con consultazioni «in strea-

ming in diretta»²⁸. Ancora non si coglie il confine fra zelo nell'adempire ed opportunità di dare ampia risonanza mediatica alle criticità della pronuncia. I gruppi di esperti poi, come a tutti è noto, non sono organismi neutri, tutto dipende dalla composizione degli stessi²⁹. In proposito è chiaro che ogni impresa ha il diritto di rivolgersi agli esperti che ritiene più adeguati a far fronte alle proprie esigenze, se però gli esperti vengono presentati come garanzia di terzietà ed imparzialità, allora occorre anche qui adottare forme di selezione trasparente e volte ad evitare cointeressenze, presenti o pregresse. L'intera vicenda, guardando in specie al rapporto fra decisione ed azioni conseguenti in capo a Google, pone dunque al giurista un interrogativo di fondo circa i reali margini di efficacia esistenti in capo alla Corte di Giustizia nei confronti dei c.d. *big player*. E qui va notata la sottile, ma rilevante, differenza che passa fra chi semplicemente è un colosso imprenditoriale (si pensi al passato caso Microsoft) e chi, oltre ad esser tale, fonda parte della sua forza anche sulla possibilità di interagire quotidianamente con miliardi di soggetti, di abilitarli a diverse funzionalità della loro interazione *online* ed *offline*, di essere in ultima istanza parte della loro esperienza quotidiana e fonte di diversi benefici. Tutto questo poi sia aggiunge al più tradizionale attivismo di impresa, capace di generare durature sinergie con il mondo politico ed accademico, nonché con una miriade di comitati ed associazioni dalle finalità più disparate e non di rado lobbistiche. In una strategia globale tutti questi fattori, opportunamente gestiti, possono giocare un ruolo decisivo nell'incidere sulle politiche comunitarie e sull'efficacia che può avere una decisione della Corte di Giustizia. Occorre dunque chiedersi se, a fronte del gigantismo di alcuni *big players*, la forza dei grandi numeri possa essere usata contro la regola di diritto affermata da una decisione. A riguardo può essere osservato come non si tratti di un fenomeno nuovo, non essendo la prima volta che il potere economico si scontra con le posizioni delle autorità comunitarie, ma proprio il passaggio dal mero scontro sul piano economico e politico istituzionalizzato (i.e. lobbying) ad un'azione orientata direttamente ai cittadini secondo il paradigma della società del web 2.0 pare segnare una discontinuità. In merito è già emersa la capacità di indirizzare l'opinione pubblica con adeguate forme di comunicazione o con strategie operative, secondo questo nuovo modello, nello scontro sui progetti SOPA (Stop

²⁸ Cfr. <https://www.google.com/advisorycouncil/> [consultato il 30/09/2014].

²⁹ Nel caso di specie non figura ad esempio fra gli esperti uno dei più noti giuristi che, ormai anni or sono, pose il problema della cancellazione delle informazioni nel contesto digitale, cfr. V. MAYER-SCHÖNBERGER, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009.

Online Piracy Act) and the PIPA (Protect IP Act) del governo statunitense. Oggi però, sui temi qui in esame, gli interessi propri dell'impresa ed i diritti degli utenti della rete non paiono essere dalla medesima parte e, pur ammettendo un impegno in favore della libertà di espressione in capo a Google (si veda l'opposizione alle politiche di censura in Cina) va altresì riconosciuto come nel caso di specie la tutela della libertà di espressione trascolori altresì nella tutela del proprio modello di *business*³⁰.

4. Una proposta de jure condendo

Come accennato nel paragrafo precedente, la peculiarità delle fattispecie in esame è data dal contrasto fra il rapporto bilaterale che caratterizza l'esercizio del diritto di cancellazione, coinvolgente l'interessato ed il titolare del trattamento, ed il rapporto multi-laterale su cui incide il processo di rimozione dei contenuti, cui prendono parte anche il fornitore del contenuto rimosso e la collettività in genere³¹. A ciò si aggiunga che, mentre nel primo caso è possibile attuare una ben precisa pretesa giuridica, riguardo al secondo rapporto né il fornitore di contenuti né la collettività possono vantare una pretesa giuridicamente rilevante verso un soggetto privato quale il gestore del motore di ricerca, che non ha obbligo alcuno di indicizzare qualsiasi contenuto disponibile *online*, salvi i limiti di comportamenti rilevanti sul piano concorrenziale³². Non è dunque forse un caso che i garanti di diversi Paesi abbiano risolto le vicende in

³⁰ Cfr. E. MOROZOV, *Google Says We Have a «Right to Know», But Really Just Wants the Right to Profit From Your Personal Information*, in *New Republic*, in [ht-tp://www.newrepublic.com/article/117844/googles-right-know-vs-europes-right-beforgotten](http://www.newrepublic.com/article/117844/googles-right-know-vs-europes-right-beforgotten) [consultato il 30/09/2014]. Cfr. anche P. DE HERT, V. PAPA-KONSTANTINOU, *How the European Google Decision May Have Nothing To Do With a Right to Be Forgotten*, in *Privacy Perspectives*, 19/06/2014, in https://www.privacyassociation.org/privacy_perspectives/post/how_the_european_google_decision_may_have_nothing_to_do_with_a_right_to_be [consultato il 30/09/2014] («Google does not express an opinion - nor may what it does be considered journalism. It only brings up information, perhaps enabling others to express an opinion [...]. Google is an accessory, not required but certainly facilitating, to the freedom of expression - and to a bunch of other freedoms as well. However, to our knowledge at least, there is to-date no such thing as protected secondary exercise of human rights - although there appears to exist secondary copyright infringement. Until that time, enabling tools have nothing to do with the freedom or rights per se»).

³¹ Quest'ultima in termini di maggiori difficoltà all'accesso alle informazioni.

³² Va inoltre ricordato come l'indicizzazione dei contenuti da parte di Google non avvenga sulla base di un algoritmo pubblicamente noto.

materia di diritto all'oblio ed alla cancellazione agendo direttamente su coloro i quali avevano pubblicato le notizie oggetto di controversia e solo indirettamente sul motore di ricerca, imponendo ai primi di non rendere indicizzabili i contenuti meritevoli di tutela e raggiungendo in tal modo un equo bilanciamento di interessi³³. Tale approccio, come la più generale esperienza giurisprudenziale inerente il rapporto fra *media* e tutela della persona, sottolineano la centralità del metodo del bilanciamento degli interessi³⁴ e del principio di proporzionalità³⁵. Va inoltre rilevato come non possa essere caricato sull'interessato tutto il peso di ricercare e chiedere la rimozione delle informazioni disponibili in Rete dove la riproducibilità dei contenuti è la norma. Dove v'è il rischio concreto di amplificare a dismisura nello spazio e nel tempo la visibilità di una notizia e dove la dimensione globale può rendere assai difficile la tutela nel caso di contenuti riprodotti in Paesi al di fuori dell'Unione, talora anche ad opera di soggetti difficilmente identificabili³⁶. Rispetto a tale contesto è inevitabile che l'interessato reclami una diversa, più estesa ed incisiva tutela rispetto alla memoria della Rete.

Per converso, la rimozione di contenuti, specie quando riguarda i *media online*, va accuratamente bilanciata con la libertà di informazione e di essere informati. Ad oggi tale bilanciamento non pare del tutto agevole, stante il quadro normativo delineato dalla dir. 95/46/EC. In proposito occorre tuttavia ricordare come la direttiva risalga ad un'epoca profondamente diversa dalla presente in termine di diffusione ed utilizzo delle reti di comunicazione elettronica³⁷. In particolare l'esistente quadro normativo porta necessariamente a scindere i due rapporti delineati all'inizio del presente paragrafo, mentre la peculiarità delle fattispecie in esame dovrebbe indurre ad esaminarli in maniera congiunta. Nello specifico pare corretta la qualificazione del gestore del motore di ricerca quale titolare del trattamento asserita dalla Corte, con il relativi corollari in termini di esercizio del diritto di rettifica e cancellazione in capo agli interessati. Le criticità concernono però la regola operativa, che esclude dalla dinamica volta alla

³³ Cfr. Opinion of Advocate General Jääskinen, cit., §§ 41-42.

³⁴ Cfr. G. FINOCCHIARO, *Il invitato di pietra nella recente sentenza Google della CGUE del 13 maggio 2014: il diritto all'identità personale*, in *giustiziacivile.com*, 21 giugno 2014.

³⁵ Tale centralità pare essere stata colta dal legislatore comunitario nell'avanzare la proposta di riforma della *data protection*. Cfr. art. 17 (3) (a) proposta di regolamento comunitario in materia di tutela dei dati personali.

³⁶ Cfr. Opinion of Advocate General Jääskinen, cit., § 44.

³⁷ Cfr. in tal senso anche Opinion of Advocate General Jääskinen, cit., §§ 10, 26-27, 61, 78.

rimozione gli altri soggetti (fornitore del contenuto rimosso e utenti) che vantano interessi autonomi inerenti agli ambiti del diritto ad informare e ad essere informati. Non pare infatti oggetto di discussione, specie in Europa, la necessità di affermare soluzioni nell'ambito dell'attività dei *media* che concilino il diritto all'oblio del singolo con il diritto alla conoscenza storica delle vicende³⁸, laddove l'oblio concerne il rischio di indebita rievocazione della vicenda e non la rimozione della stessa dalla conoscenza storica³⁹. Diversamente, le criticità emergono laddove sul piano operativo la rimozione dei contenuti ad opera del gestore del motore di ricerca su istanza dell'interessato, benché in conformità al vigente quadro normativo, avviene in maniera non adeguatamente calibrata rispetto alla valutazione delle potenziali ricadute sulla libertà di espressione.

Nello specifico, come rilevato in precedenza⁴⁰, non può in prima battuta essere un soggetto privato a porre in essere un bilanciamento di interessi rispetto al quale non ha le capacità e competenze necessarie. Non può un motore di ricerca conoscere nel dettaglio le vicende, valutare il delicato bilanciamento di interessi e rendere una sorta di universale⁴¹ giudizio su cosa debba essere o non essere reso pubblico. A riguardo la Corte ha tentato di conciliare quanto, nel vigente contesto normativo, pare difficilmente conciliabile, facendo esplicito riferimento alla possibilità di adire le *data protection authorities*. Tuttavia, stante la natura individuale del diritto in questione, specie laddove il gestore del motore di ricerca decida di dar corso autonomamente alla richiesta dell'interessato, il titolare del sito web rimane del tutto estraneo alla vicenda⁴², né — per quanto detto

³⁸ Cfr., con riguardo all'esperienza italiana, Cass., sez. III, 5 aprile 2012, n. 5525, in *Nuova giur. civ. comm.*, 2012, I, pp. 836 ss., con nota di A. Mantelero; G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. Inf.* 2010, pp. 391 ss.; T.E. FROSINI, *Il diritto all'oblio e la libertà informatica*, ibid., 911; A. DI MAJO, *Il tempo siamo noi...*, in *Corr. giur.*, 2012, pp. 769 ss.; F. DI CIOMMO-R. PARDOLESI, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!*, in *Danno e resp.*, 2012, pp. 701 ss.

³⁹ Cfr. più diffusamente A. MANTELERO, *Right to be forgotten ed archivi storici dei giornali. La Cassazione travisa il diritto all'oblio*, in *Nuova giur. civ. comm.*, 2012, I, pp. 543-549.

⁴⁰ Cfr. *supra* par. 3.

⁴¹ Questo almeno in una prospettiva europea, posto che Google detiene il 90% del mercato dei motori di ricerca nell'UE.

⁴² Cfr. J. ZITTRAIN, *The right to be forgotten ruling leaves nagging doubts*, in *Financial time*, July 13, 2014 («But here state power is being exercised without the involvement of the state: Google decides how to handle redaction requests. If a search engine declines to alter its results, the claimant might appeal to a national data protection authority. But if the request is agreed to, there is no mechanism for review. Under the court's decision, the

in precedenza — ha alcun titolo per poter adire l'autorità giudiziaria ed ottenere il ripristino dell'indicizzazione. Il quadro si presenta dunque come complesso e necessita di un'opportuna soluzione *ad hoc* che tenga conto della peculiarità dell'interazione esistente fra attività dei motori di ricerca, diritti degli interessati, fornitore di contenuti ed interesse collettivo alla conoscenza delle informazioni. Tuttavia proprio il contemperamento di tali diversi interessi, anche in ragione del rango degli stessi, richiede la definizione di un modello di rimozione basato su decisioni adottate dalle autorità garanti o dalle corti, in cui il bilanciamento di interessi così rilevanti non è affidato al giudizio di un'impresa privata. In tal senso, si possono delineare tre diverse soluzioni normative volte a garantire l'esercizio del diritto di cancellazione nelle fattispecie in esame: I. introduzione di un obbligo di esercitare tale diritto non verso il titolare in via stragiudiziale, ma solamente mediante ricorso alle autorità garanti o alle corti; II. adozione di un modello analogo al *notice and take down* esistente per i contenuti protetti da privative; III. definizione di una modalità specifica per l'esercizio del diritto di rettifica/cancellazione rispetto ai motori di ricerca. Delle tre opzioni la terza pare la più adeguata. La prima infatti creerebbe un'anomalia rispetto al quadro normativo delineatosi con riguardo all'esercizio dei diritti dell'interessato, inducendo un'eccezione difficilmente armonizzabile.

Sul piano pratico, va poi considerata la potenziale numerosità delle richieste, che potrebbe indurre se non la paralisi, quantomeno un forte rallentamento dell'attività delle autorità garanti. La seconda opzione, non di rado invocata a prova della semplicità di attuazione della pronuncia in esame, non tiene tuttavia conto della differenza che intercorre fra i diritti d'autore ed i diritti della personalità, in termini di diversa complessità dell'accertamento delle violazioni. Per tali motivi, come cennato, la terza via sembra essere la più percorribile, sebbene possa mettere in crisi l'approccio tecnologicamente neutro della regolamentazione europea in materia di *data protection*; tuttavia proprio tale approccio pare già meritevole di riconsiderazione per altre ragioni (es. adozione di soluzioni *ad hoc* per i *Big Data analytics*). Nello specifico la soluzione potrebbe essere offerta da una procedura che mantenga in capo all'interessato la possibilità di esercitare il proprio diritto nei confronti del motore di ricerca, ma nel contempo induca necessariamente al coinvolgimento delle autorità giudicanti. L'interessato potrebbe così far valere il proprio diritto alla cancellazione

public's right to know is to be balanced against a claimant's right to privacy - but there is no easy way for the public to remonstrate against poor balancing.»).

nei confronti del motore di ricerca titolare del trattamento e, a fronte di tale richiesta, quest'ultimo dovrebbe porre in essere una mera sospensione temporanea della visibilità del *link*, dandone notizia all'utente ed al titolare del sito web⁴³. Entro un breve termine di decadenza (es. 30 giorni) l'interessato dovrebbe poi adire le autorità giudicanti competenti per far valer il proprio diritto a alla cancellazione. Le corti adite o le autorità garanti, ove accolgano l'istanza, ordineranno al sito ospitante i contenuti di rendere quest'ultimi non indicizzabili. Laddove invece tale provvedimento possa risultare poco efficace, specie in relazione ai sopra menzionati profili giurisdizionali e di *enforcement*, l'autorità adita potrà richieder direttamente al motore di ricerca di rimuovere il contenuto dai risultati delle ricerche, ma in tal caso sarà tale autorità a porre in essere il necessario bilanciamento degli interessi contrapposti. Laddove infine l'interessato omettesse di agire entro il termine di decadenza di cui sopra, il motore di ricerca provvederà a rendere nuovamente disponibili fa i propri risultati le informazioni che sono state oggetto di contenzioso. Il ricorso all'autorità fungerebbe poi da filtro rispetto alla fondatezza delle domande, almeno in maniera maggior di quanto non accada con la semplice compilazione di un modulo *online* quale quello predisposto da Google a valle della pronuncia in esame. L'efficacia di tale filtro andrebbe poi rafforzandosi con il progressivo formarsi della giurisprudenza in tema.

5. Conclusione: oltre il caso Google

Nel concludere queste brevi note sul caso Google, seguendo l'impostazione adottata volta ad indagare più le implicazioni sugli scenari futuri della pronuncia che gli aspetti tecnici della stessa—quest'ultimi oggetto di altri contributi nel presente volume —,pare opportuno collocare la decisione in un più ampio contesto che comprende anche la recente pronuncia sulla *data retention*⁴⁴ e, guardando al di là dell'Atlantico la deci-

⁴³ Cfr. J. ZITTRAIN, *The right to be forgotten ruling leaves nagging doubts*, cit. («Thus website owners can stand in for the public, objecting to overly broad takedowns so long as they know that they are taking place - and Google's decision to notify them is vital to achieving the court's stated purpose»).

⁴⁴ Cfr. Corte Giustizia UE, 8 aprile 2014, cause riunite C 293/12 e C 594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General*, con l'intervento dell'Irish Human Rights Commission, e Kärntner

sione della Corte Suprema statunitense⁴⁵ che ha disposto che polizia non possa, senza mandato, estrarre informazioni dal cellulare di un soggetto in stato di arresto. La disamina e la correlazione fra tali pronunce non è certo tema da affrontarsi in brevi note conclusive, quello che invece si vuole qui sottolineare è l'emergere, tanto nell'UE, quanto negli USA, di una sorta di contro-onda rispetto all'orientamento che ha caratterizzato gli ultimi lustri. Diverse esigenze, o giustificazioni, hanno infatti indotto ad approvare normative che hanno esteso la capacità di controllo in capo ai soggetti pubblici, soprattutto alla luce della sinergia fra pubblico e privato caratterizzante le moderne forme di sorveglianza sociale. Estese raccolte di dati, obblighi di conservazione delle informazioni nel tempo, uniti a poteri di indagine e di accesso in capo alle autorità pubbliche, hanno creato un contesto in cui i cittadini hanno perso la percezione del confine fra la raccolta dei loro dati per scopi commerciali ed il riuso degli stessi per diverse finalità di controllo o monitoraggio sociale. Di questa strategia, come ormai noto, hanno fatto parte anche le imprese private, la cui promozione di un modello incentrato sull'accesso alle informazioni dell'utente era in linea con gli intenti dei governi, che a tali ricchi forzieri di dati potevano accedere in varia maniera e solitamente all'insaputa degli interessati e della collettività in generale. In questo più vasto panorama, il diritto alla cancellazione non è più dunque solo il soddisfacimento dell'interesse di un singolo, ma diviene un tassello di una più ampia e, auspicabilmente, nuova strategia che potrebbe portare ad un ecosistema meno connotato da un'eccessiva raccolta di dati personali. La necessità di un simile mutamento è oggi tanto più avvertita, a fronte dei nuovi scenari aperti dai *Big Data analytics* che, per converso, incrementano i rischi di un monitoraggio esteso ed invasivo.

Abstract

The decision of the European Court of Justice on the right to be forgotten seems to be oriented to anticipate some aspects of the ongoing reform of the EU

Landesregierung v Michael Seitlinger, Christof Tschohl and others, in <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=128869> [consultato il 30/09/2014].

⁴⁵ Cfr. *Riley v. California*, 573 U.S. (25/06/2014), in http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

data protection and to reopen the discussion on the right to erasure. In the same way, the «reaction» adopted by Google intends to point out the criticisms related to the decision, in the light of the future regulation. The solutions suggested by the court are consistent with the existing legal framework, but not adequate with regard to the state-of-the-art.

For this reason, the future regulation should consider the peculiar nature of the search engine as data controller. From this perspective, a potential solution is represented by a specific provision that introduces a temporary removal of the link from the list of results, on the basis of the data subject's request. If, in a given lapse of time, the data subject does not make a legal action, the link is reactivated

Salvatore Sica-Virgilio D'Antonio

La procedura di de-indicizzazione

SOMMARIO: 1. Premessa - 2. La richiesta di rimozione nell'impalcatura della decisione - 3. L'oggetto dell'istanza: il diritto alla de-indicizzazione - 4. Le parti del procedimento: l'interessato/istante ed i 'controinteressati' - 5. Il ruolo 'ibrido' del gestore del motore di ricerca - 6. Il procedimento di *notice and take down* del DMCA: un modello possibile? - 7. L'ordinamento italiano e l'orientamento di Cass. n. 5525/2012 - 8. Conclusioni

1. Premessa

Milan Kundera scrive che *«l'oblio ci riconduce al presente»* perché *«occorre dimenticare per rimanere presenti, dimenticare per non morire, dimenticare per restare fedeli»*¹. In effetti, provando a forzare un po' il senso ultimo del passaggio dello scrittore ceco, l'oblio, soprattutto allorché declinato in termini di diritto, pare stagliarsi, oggi, come uno dei principali temi del tempo presente. La tensione degli individui nella ricerca della 'dimenticanza' non tanto di sé, ma di 'qualcosa di sé', finalizzata che sia a 'rimanere presenti' (cancellando episodi incompatibili con il proprio essere attuale), a 'non morire' (magari nell'identità pubblica faticosamente alimentata) o a 'restare fedeli' (eliminando dal *public eye* 'cambiamenti di rotta', piccoli o grandi, ideologici o di altra natura), si è esasperata negli ultimi anni, quasi a far da contraltare al (presunto) 'eterno attuale' connaturato in Internet. In buona sostanza, come sovente accade nell'evoluzione del discorso giuridico, il dibattito intorno alla stessa esistenza di un vero e proprio diritto all'oblio si consolida – e, per certi versi, siffatta prerogativa dell'individuo viene ipotizzata come esistente – nel momento stesso in cui ne è posta in discussione la sostanza in ragione del rischio insito nel perenne presente promesso dalla Rete ed identificato come uno dei tratti

* Lo scritto, pur unitariamente concepito dai due Autori, deve così essere attribuito nelle sue singole parti: S. Sica, par.6/7 - V. D'Antonio, par. 1/5 - 8.

¹ I riferimenti presenti nel testo sono tratti da *'La lenteur'*, romanzo edito nel 1995 e pubblicato in Italia, nel medesimo anno, con il titolo *'La lentezza'* (trad. di Ena Marchi).

caratterizzanti del *medium*².

D'altronde, se un utente si avventura nel *web*, oggi, alla ricerca della parola 'oblio' utilizzando i principali motori di ricerca disponibili, molti dei risultati che otterrà assoceranno il termine con un richiamo al diritto ed, in molti casi, a quello che è, allo stato, il punto di riferimento indiscusso del dibattito in tema: la sentenza della Grande Sezione della Corte di giustizia dell'Unione Europea dello scorso 13 maggio 2014 (resa nella causa C-131/12)³. La circostanza di siffatto quadro di risultati, indotto dal *battage* mediatico che ha accompagnato la decisione, è curiosa per l'osservatore e, per certi versi, emblematica dello stesso fenomeno di cui stiamo discorrendo, ove si pensi che la locuzione di 'diritto all'oblio' non compare pressoché mai nel testo della decisione, ma anzi viene utilizzata con parsimonia estrema e, quasi, in maniera fugace⁴.

Il vero oggetto della sentenza, infatti, è quello che, al più, può essere considerato un 'frammento' particolare e marginale del diritto all'oblio: il diritto all'oscuramento di determinati risultati di ricerca associati al proprio nome dalle *search engine technologies*, cioè una moderna prerogativa propria ed esclusiva dei rapporti tra internauti e gestori dei motori di ricerca.

² Nel contesto di un dibattito, da sempre, particolarmente vivace, si rinvia a G.B.FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, I, 1990, pp. 801 ss.; V.ZENOVICH, voce *Identità personale*, in *Dig. disc. priv.*, sez. civ., IX, Torino, 1995, pp. 295 ss.; P.BERNAL, *The EU, the US and Right to be Forgotten*, in S.GUTWIRTH – R.LEENES – P.DE HERT (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, Springer, 2014, pp. 61 ss., e G.FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. Inf.* 2010, pp. 391 ss. ed agli ampi riferimenti bibliografici *ivi* richiamati. Vedi anche G.RESTA, *Identità personale e identità digitale*, in *Dir. Inf.* 2007, pp. 511 ss.

³ Tra i primi commenti organici alla decisione, si veda A.PALMIERI – R.PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quad. Foro it.*, 1, 2014, 1 ss. Ad ogni modo, già sulle conclusioni dell'Avvocato generale Nillo Jääskinen, seppur caratterizzate da una lettura della fattispecie ispirata a soluzioni decisamente più moderate rispetto a quelle poi confluite nella sentenza, si veda D.LINDSAY, *The «right to be forgotten» in European data protection law*, in N.WITZLEB – D.LINDSAY – M.PATERSON – S.RODRICK (eds.), *Emerging Challenges in Privacy Law. Comparative Perspectives*, Cambridge, 2014, pp. 290 ss.

⁴ Precisamente, la parola 'oblio' compare soltanto quattro volte nel corpo della sentenza ed articolata nella locuzione 'diritto all'oblio' appena due, ai paragrafi 20 e 91.

2. La richiesta di rimozione nell'impalcatura della decisione

Il momento fondativo dell'intera impostazione decisionale della sentenza della Corte di giustizia si identifica facilmente nella qualificazione dell'attività dei motori di ricerca operanti nel *web*⁵ quale «*trattamento di dati personali*», ai sensi dell'art. 2, lett. b), della Direttiva 95/46/CE⁶.

Da siffatto assunto discende, infatti, la conseguente attribuzione al gestore del motore di ricerca, che opera il trattamento, della qualità di «*responsabile*» dello stesso, ai sensi dell'art. 2, lett. d), del medesimo testo normativo, in quanto soggetto che determina le finalità e gli strumenti dell'attività di organizzazione ed aggregazione di informazioni pubblicate su Internet. Il gestore, pertanto, è chiamato ad assicurare, nell'ambito delle proprie responsabilità, competenze e possibilità, la conformità del proprio *agere* alle previsioni della direttiva 95/46, con correlato diritto degli interessati dal trattamento di rivolgersi direttamente al responsabile dello stesso affinché sia pienamente tutelato il loro diritto al rispetto della sfera privata. E ciò, peraltro, in maniera del tutto autonoma rispetto ai rapporti intercorrenti tra interessato e titolare del sito sorgente, ove l'informazione è contenuta: la richiesta rivolta al motore di ricerca prescinde dalla differente istanza di cancellazione eventualmente proposta al soggetto che ha caricato l'informazione *on-line*. La linea di cesura interpretativa segnata dalla sentenza è rappresentata, dunque, dalla scelta di investire di indipendenza il servizio svolto dai motori di ricerca, inteso come autonomo trattamento dei dati personali, distinguendolo da quello proprio dei gestori delle pagine sorgente. In questo segmento deve, poi, leggersi il riconoscimento in capo al gestore del motore di ricerca della posizione di responsabile dell'autonomo trattamento⁷.

⁵ Nel corpo della decisione quella dei motori di ricerca viene definita come attività «*consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza*» (cfr. paragrafi 21 e 41). Siffatta attività, secondo la Corte di giustizia, è qualificabile come trattamento di dati personali allorché le informazioni poste a disposizione degli utenti del *web* contengano dati personali.

⁶ Vedi E.KOSTA – CH.KALLONIATIS – L.MITROU – E.KAVAKLI, *Search Engines: Gateway to a New «Panopticon»?*, in S.FISCHER-HÜBNER – C.LAMBRINOUDAKIS – G.PERNUL (eds.), *Trust, Privacy and Security in Digital Business*, Springer, 2009, 14 ss. Cfr. anche, di recente, i contributi presenti in S.FURNELL – C.LAMBRINOUDAKIS – J.LOPEZ (eds.), *Trust, Privacy, and Security in Digital Business - 10th International Conference*, 2013, Prague, Czech Republic, August 28-29, 2013, Springer, 2013.

⁷ Opportunamente A.PALMIERI – R.PARDOLESI, *Dal diritto all'oblio all'occultamento in*

La Corte, tramite questa soluzione interpretativa, giunge a riconoscere a qualsivoglia interessato il diritto di presentare al gestore del motore di ricerca istanze ai sensi degli artt. 12, lett. b), e 14, co. 1, lett. a), della direttiva 95/46⁸ finalizzate ad ottenere l'esclusione dai risultati di ricerca collegati al proprio nome di determinate informazioni presenti in Rete e riguardanti la sua sfera personale. Nell'impalcatura della decisione, il primo vaglio di fondatezza dell'istanza è rimesso proprio al gestore del motore di ricerca, chiamato al difficile compito di identificare il giusto equilibrio tra i diritti fondamentali della persona, derivanti dagli artt. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea, ed il (potenzialmente configgente) legittimo interesse degli utenti di Internet intenzionati ad avere accesso a quella data informazione⁹. L'interessato, ove veda disattesa la propria istanza dal gestore del motore di ricerca, può rivolgersi all'autorità di controllo nazionale in materia di *privacy* o, in alternativa, all'autorità giudiziaria, affinché queste – quasi a guisa di organi di secondo grado – verifichino la correttezza della posizione assunta dal responsabile del trattamento ed, eventualmente, ordinino allo stesso l'adozione di misure precise conseguenti¹⁰. Tramite il ricorso al Garante nazionale o all'autorità giudiziaria, pertanto, l'interessato, facendo accertare la violazione dei propri diritti o, comunque, la prevalenza degli stessi sul diritto alla conoscenza degli utenti del web, potrà cercare di ottenere

rete, cit., 6, sottolienano come, rispetto a questo specifico profilo, la Corte entri in contraddizione anche con la ricostruzione offerta dal Gruppo di lavoro Articolo 29 nel parere n. 1/2008, secondo cui i motori di ricerca, «*as providers of content data (such as the data in the index), generally [...] are not to be held as primarily responsible under European data protection law for the personal data they process. Exceptions are the availability of a long-term 'cache' and value added operations on personal data (such as search engines aimed at building profiles of natural persons)*». I due Autori segnalano la disponibilità del documento menzionato all'indirizzo http://ec.europa-.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [consultato il 30/09/2014].

⁸ Al par. 77 della decisione.

⁹ Cfr. par. 81 della decisione in commento.

¹⁰ Il par. 82 della decisione prevede esplicitamente che «*l'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di applicazione degli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46, da effettuarsi allorché ricevono una domanda quale quella oggetto del procedimento principale, possono ordinare al suddetto gestore di sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona, senza che un'ingiunzione in tal senso presupponga che tale nome e tali informazioni siano, con il pieno consenso dell'editore o su ingiunzione di una delle autorità sopra menzionate, previamente o simultaneamente cancellati dalla pagina web sulla quale sono stati pubblicati*».

quanto negato in prima istanza dal gestore del motore di ricerca, cioè la cancellazione, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal proprio nome, dei link verso pagine web pubblicate da terzi e contenenti informazioni a sé relative.

Tale risultato prescinde completamente dalla cancellazione dalla Rete della medesima pagina ove le informazioni sono state pubblicate in origine o di altri *link* che comunque alle stesse rimandino¹¹. In definitiva, la Corte di giustizia, con la qualificazione quale trattamento di dati personali delle operazioni di ricerca ed organizzazione dei risultati proposti dai gestori di *search engine*, pone le basi per l'applicabilità agli stessi dell'intero corpo disciplinare proprio della direttiva 95/46/CE ed, in particolare, dei meccanismi di esercizio dei diritti degli interessati previsti dalla normativa comunitaria (cioè istanza al responsabile del trattamento e, in seconde cure, ricorso al Garante o all'autorità giudiziaria)¹². Con la sentenza pronunciata nel caso C-131/12, in ultima analisi, la Corte di giustizia ha inteso definire una serie di principi di diritto, centrati sul rapporto intercorrente tra individui, dati personali e motori di ricerca, con immediate ricadute sul piano dell'ampliamento delle posizioni giuridiche proprie dei soggetti che risiedono in uno dei paesi dell'Unione. Nella prospettiva specifica delle procedure di notifica e rimozione dei contenuti nell'ambito del c.d. *web 2.0*, le soluzioni apprestate dalla Corte possono essere così rilette e sintetizzate: *a*) ogni cittadino comunitario può richiedere direttamente al motore di ricerca la soppressione di un collegamento ad una pagina *web* che contenga dati personali ad esso riferibili, anche se pubblicati lecitamente nella pagina sorgente; *b*) il prestatore, nelle vesti di responsabile del trattamento, è tenuto a valutare l'istanza del privato ed, in caso di rigetto (o di mancato riscontro), quest'ultimo potrà adire l'Autorità amministra-

¹¹ In tema, si rinvia alle riflessioni di C.BENNETT – CH.PARSONS – A.MOLNAR, *Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice*, in S. GUTWIRTH – R.LEENES – P.DE HERT (eds.), *Reloading Data Protection*, cit., pp. 41 ss.

¹² Prima della decisione in commento, uno dei precedenti più rilevanti della Corte di giustizia in materia di *privacy on-line* è stato quello inerente il cd. 'caso Lindqvist': CGE, 6 novembre 2003, causa C-101/01, in *Foro it.*, 2004, IV, pp. 57 ss., con nota di A.PALMIERI – R.PARDOLESI, *Il codice in materia di protezione dei dati personali e l'intangibilità della privacy comunitaria*; in *Giur. it.*, 2004, pp. 1805 ss., con nota di G.CASSANO – I.P. CIMINO, *Qui, là, in nessun luogo ... - Come le frontiere dell'Europa si aprirono ad Internet: cronistoria di una crisi annunciata per le regole giuridiche fondate sul principio di territorialità*, ed in *Danno e resp.*, 2004, pp. 382 ss., con note di A.GIANNACCARI, *Il trasferimento di dati personali in Internet*, ed T.UBERTAZZI, *Sul bilanciamento tra libertà di espressione e privacy*.

tiva indipendente o quella giudiziaria; c) l'attività di bilanciamento dovrà essere svolta tenendo in giusta considerazione la libertà di impresa del *provider* ed i diritti di accesso all'informazione di tutti i consociati, posto comunque che, in linea generale, è preminente il diritto dell'interessato a vedere deindicizzati i risultati considerati contrari al proprio diritto alla riservatezza, alla tutela dei dati personali ed, ancora, all'identità personale, anche in assenza di un effettivo pregiudizio. In tal senso, è da rilevare come il disegno della Corte di giustizia, per certi versi, vada anche oltre quanto, ad oggi, previsto nel testo della proposta di Regolamento sulla protezione dei dati, presentata dal Parlamento europeo e dal Consiglio nel 2012 e in via di approvazione in seno all'ampio processo di revisione ed aggiornamento della direttiva 95/46/CE¹³. Difatti, la previsione dell'art. 17 della proposta di Regolamento, rubricato «*Diritto all'oblio e alla cancellazione*»¹⁴, al paragrafo 3, limita l'obbligo di cancellazione posto in capo al responsabile del trattamento nei casi in cui la conservazione dei dati personali sia necessaria per l'esercizio del diritto alla libertà d'espressione connesso all'attività giornalistica, per motivi di interesse pubblico nel settore della sanità pubblica, per finalità storiche, statistiche o di ricerca scientifica o ancora per adempiere un obbligo legale di conservazione di dati personali previsto dal diritto dell'Unione. La posizione giuridica tratteggiata dalla Corte di giustizia parrebbe addirittura estranea a siffatti confini e rimessa

¹³ Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 final, in www.ec.europa.eu.

¹⁴ La previsione richiamata nel testo, in particolare, ai paragrafi 3 e 4, prevede che « *il responsabile del trattamento provvede senza ritardo alla cancellazione, a meno che conservare i dati personali non sia necessario: (a) per l'esercizio del diritto alla libertà di espressione in conformità dell'articolo 80; (b) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 81; (c) per finalità storiche, statistiche e di ricerca scientifica in conformità dell'articolo 83; (d) per adempiere un obbligo legale di conservazione di dati personali previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento; il diritto dello Stato membro deve perseguire un obiettivo di interesse pubblico, rispettare il contenuto essenziale del diritto alla protezione dei dati personali ed essere proporzionato all'obiettivo legittimo; (e) nei casi di cui al paragrafo 4. 4. Invece di provvedere alla cancellazione, il responsabile del trattamento limita il trattamento dei dati personali: a) quando l'interessato ne contesta l'esattezza, per il periodo necessario ad effettuare le opportune verifiche; b) quando, benché non ne abbia più bisogno per l'esercizio dei suoi compiti, i dati devono essere conservati a fini probatori; c) quando il trattamento è illecito e l'interessato si oppone alla loro cancellazione e chiede invece che ne sia limitato l'utilizzo; d) quando l'interessato chiede di trasmettere i dati personali a un altro sistema di trattamento automatizzato, in conformità dell'articolo 18, paragrafo 2* ».

esclusivamente alla ‘rappresentazione di sé’ che, nel tempo, l’interessato intenda cristallizzare nella memoria del *web*.

3. *L’oggetto dell’istanza: il diritto alla de-indicizzazione*

Si è detto come la decisione della Corte di giustizia, pur additata quale punto di svolta del diritto all’oblio in Internet, menzioni soltanto fugacemente siffatta posizione giuridica, per soffermarsi piuttosto su una sorta di più neutro e più tecnico «diritto a non essere trovati facilmente»¹⁵ dagli internauti che interrogano i motori di ricerca: in sostanza, si tratta del diritto alla de-indicizzazione di determinate pagine *web* a fronte di specifici parametri di ricerca (cioè il nome dell’interessato/istante). La segnalata ritrosia della Corte nel far riferimento esplicito al diritto all’oblio nel corpo della decisione non si ritiene casuale: con buona probabilità, la *Grande Chambre* non aveva in animo di definire lo stato dell’arte del *right to be forgotten* al tempo di Internet, bensì di disciplinare una posizione giuridica che, pur all’oblio connessa, presenta tratti di indubbia peculiarità in quanto specifica dei rapporti tra individui e motori di ricerca che scandagliano costantemente la Rete. Si tratta, appunto, del diritto alla dis-associazione del proprio nome da un dato risultato di ricerca.

Secondo la Corte i dati personali, allorché filtrati attraverso il processo di indicizzazione proprio dei motori di ricerca, vengono investiti da un potente effetto comunicativo, assolutamente pregnante e differente rispetto alla visualizzazione ‘semplice’ della pagina da cui essi provengono, con il risultato ultimo di creare così un autonomo e delicato comparto.

La ricerca di collegamenti a pagine *web* riferibili ad un nome viene equiparato, rileggendo il corpo della sentenza, ad una modalità di creazione di un ‘profilo’ di un determinato soggetto: l’estrema genericità del trattamento svolto dai motori di ricerca, al quale non è stato in via generale riconosciuto dalla Corte alcuno scopo giornalistico, storico o statistico, conduce alla previsione di una sorta di ‘nuovo’ diritto in capo al soggetto cui le informazioni si riferiscono. Tale posizione giuridica si concretizza nella facoltà di chiedere, in via diretta, al gestore della piattaforma la rimozione di quei collegamenti *web* ritenuti lesivi dei propri diritti fondamentali alla riservatezza ed alla tutela dei dati personali. Così come

¹⁵ Discorrono esplicitamente di «*right not to be found easily*» A.PALMIERI – R.PARDOLESI, *Dal diritto all’oblio all’occultamento in rete*, cit., 14.

configurato dalla Corte, peraltro, quello all'oscuramento di determinati *link* si staglia come diritto estremamente pervasivo, nella misura in cui la potenziale lesione da tutelare tramite deindicizzazione non presuppone né l'illiceità dell'informazione presente sul sito sorgente, né trova necessario fondamento nella sussistenza di un pregiudizio in capo all'interessato. Anzi, nella sentenza si legge, in diversi passaggi, che il diritto alla rimozione dalle SERP (*Search Engine Result Pages*) prescinde completamente dalla verifica che l'inclusione dell'informazione in questione in siffatto elenco arrechi un pregiudizio all'interessato/istante. Ed allora, nel venire specificamente ai profili procedurali, è questo il diritto precipuo che può essere oggetto dell'istanza proposta dall'interessato al gestore del motore di ricerca: non già il diritto alla cancellazione dell'informazione dalla rete, bensì quello alla dis-associazione di una specifica pagina, identificata dal proprio *Uniform Resource Locator* (URL), da una peculiare *query* di ricerca (cioè il nome dell'interessato).

In altre parole, nel disegno della Corte di giustizia, sembrerebbe assistersi ad una sorta di 'ripensamento' del diritto all'oblio, seppur inteso nella sua accezione dinamica e 'tecnologica'¹⁶: diritto non più (o non soltanto) alla dimenticanza di sé, bensì al mero ridimensionamento della propria visibilità telematica. Si tratta, a ben vedere, di principi non sconosciuti ai media tradizionali, come, ad esempio, la stampa e gli argomenti adoperati dalla Corte a sostegno della propria ricostruzione sono vicini a quelli cui ricorre la giurisprudenza che ha sancito il divieto di ingiustificata rievocazione di fatti oramai datati ed inattuali¹⁷. Siffatti principi, tradotti nei meccanismi propri della Rete, si declinano nel senso che ciascun soggetto ha diritto a che la propria vicenda personale, non più attuale, trascorra dalla prima pagina e dagli 'strilloni' della Rete – cioè dalle SERP prodotte dai motori di ricerca – alle pagine interne o 'di nicchia' (che pure concorrono a comporre il *web*, seppure in secondo piano). Il dato personale oggetto di istanza di deindicizzazione, infatti, non viene rimosso dal *mare magnum* di dati memorizzati nel *web*, ma semplice-

¹⁶ In tema, si rinvia ancora alle riflessioni formulate da G.FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., pp. 391 ss. Vedi anche F.MANGANO, *Diritto all'oblio*, in *Giur. merito*, 2012, pp. 2621 ss.

¹⁷ Ha, di recente, ribadito siffatto principio Cass. 26 giugno 2013, n. 16111, in *Foro it.*, 2013, I, pp. 2442 ss. D'altro canto, l'attualità della notizia è da sempre uno dei parametri di valutazione, utilizzati dalla giurisprudenza di merito, per vagliare la liceità della pubblicazione: si vedano, sul punto, Trib. Roma 15 maggio 1995, in *Dir. Inf.* 1996, pp. 424 ss.; Trib. Napoli 8 aprile 1995, *ibidem*, 1995, pp. 1016 ss.; Trib. Roma 24 gennaio 1996, *ibidem*, 1996, pp. 572 ss., con nota di V.ZENO-ZENCOVICH.

mente sottratto ad una modalità di reperimento semplice ed istantanea. Eliminato il collegamento, l'utente interessato a quella data informazione potrebbe effettuare ulteriori ricerche visitando in maniera diretta le pagine e gli archivi dei quotidiani o di altre 'fonti', secondo quanto avveniva agli 'albori' di Internet. L'oggetto dell'istanza presentata al motore di ricerca, dunque, consiste nella sottrazione al pubblico di una modalità di accesso semplificata e generalizzata ad informazioni sul proprio conto, le quali, lecitamente pubblicate in tempi diversi, potrebbero comunque permanere e rimanere accessibili attraverso una più difficoltosa navigazione nel sotto-livello di fruizione rappresentato dalle pagine sorgente.

D'altro canto, proprio perché non discorriamo del diritto dell'interessato a 'scompare' dal *web*, bensì di una posizione giuridica differente, collegata alla semplice riduzione di visibilità dell'informazione presente in Rete, sarà onere dell'istante identificare analiticamente, tramite l'URL di riferimento, la pagina sorgente (o le pagine sorgente) da depennare dai risultati di ricerca collegati al suo nome. Ed ancora, visto che, per gli interessi in gioco da contemperare, non sono immaginabili istanze *omnibus*, tale procedimento andrà reiterato non soltanto per ogni pagina sorgente, bensì per ogni motore di ricerca ritenuto rilevante. Va pure detto che la sentenza della Corte di giustizia (e le prassi diffuse tramite la modulistica introdotta, ad esempio, da Google e Bing¹⁸) sembrerebbero riguardare esclusivamente quei risultati di ricerca ove si crea una associazione diretta tra nome di un individuo ed una determinata pagina sorgente. Visto che, anche dopo la deindicizzazione, l'informazione rimane comunque in Rete, all'utente, anche tramite il medesimo motore di ricerca, potrebbe essere comunque consentito di raggiungere la pagina sorgente, utilizzando forme di interrogazione del *provider* maggiormente articolate e circostanziate. In altre parole, allorché si vada oltre il rapporto di diretta associazione nome/pagina sorgente ed il collegamento sia meramente indiretto, perché la pagina sorgente compare tra i risultati soltanto a fronte di ricerche particolarmente articolate, ove il nome dell'interessato rappresenti magari soltanto una parte della *query*, allora deve ritenersi non possa più trovare applicazione il principio enunciato dalla Corte di giustizia. Questo perché la sentenza, come più volte osservato, non deve favorire forme di censura della Rete, ma rappresenta la base di principi che devono regolare la diretta associabilità di un nome ad una data pagina sorgente contenente informazioni personali. Per tal motivo, non pare possibile ipotizzare istanze di rimozione di risultati di ricerca che vadano oltre la disassociazione

¹⁸ Vedi *infra*.

di quella data pagina sorgente da quel determinato nome, sino a coprire magari tutte le possibilità di accesso alla pagina stessa, attraverso differenti modalità di interrogazione del motore di ricerca. L'attuale modulistica diffusa *on-line* dai principali operatori di mercato, d'altro canto, sembra, allo stato, andare in questa direzione, visto che all'interessato non viene concessa la possibilità di indicare sequenze di parole che, ove associate al proprio nome, conducono a risultati da rimuovere, bensì semplicemente di indicare *«il nome che, quando utilizzato come chiave di ricerca, produce una lista di risultati da cui richiede che uno o più risultati siano rimossi»*¹⁹.

4. Le parti del procedimento: l'interessato/istante e i 'controinteressati'

Definito quale sia l'oggetto dell'istanza, vi sono da prendere in considerazione le possibili parti (dirette o indirette) del procedimento di rimozione, ognuna delle quali sarà portatrice di un peculiare interesse. In effetti, l'attività di bilanciamento tra diritti ed interessi contrapposti auspicato, seppur in maniera esemplificativa, dalla Corte grava in via preliminare unicamente sulla figura del prestatore di servizi, il quale è tenuto a vagliare le istanze dei privati e, qualora ritenuto necessario, dare esecuzione alle richieste di deindicizzazione. Le posizioni giuridiche che si pongono in correlazione le une con le altre in questo particolare ambito delle funzionalità del *web*, che si staglia a sorta di diaframma tra la memorizzazione quasi permanente dei dati e delle informazioni sulle pagine 'madre' e l'accesso e la fruizione del servizio 'essenziale' di navigazione in Internet nella disponibilità degli utenti, possono essere ascritte a tre distinti gruppi, suddivisi in funzione dei soggetti coinvolti direttamente ed indirettamente dal trattamento.

Nel prendere le mosse dalla posizione dell'interessato/istante²⁰, come

¹⁹ Dal modulo diffuso da Google, reperibile alla pagina *web*: https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=it [consultato il 30/09/2014].

²⁰ V'è chiaramente un onere di identificazione, che l'istante deve assolvere attraverso l'allegazione, alla propria richiesta, di un documento di riconoscimento o attraverso strumenti di firma digitale. Evidentemente, il gestore del motore di ricerca potrà evitare di dar corso a tutte le istanze che non siano accompagnate dalla certa identificazione dell'interessato, dal momento che è più facile si tratti di *«richieste di rimozione fraudolente da parte di persone che si spacciano per altre nel tentativo di danneggiare concorrenti o di eliminare impropriamente informazioni legali»* (dal modulo *on-line* di Google). L'istanza potrebbe essere presentata anche da un rappresentante dell'interessato (o da un avvocato), ma resta ferma la necessità di allegazione del documento d'identità dell'interessato. In

ampiamente argomentato dai giudici del Lussemburgo, questi, nel proporre la propria richiesta di deindicizzazione di determinati risultati associati al proprio nome, invocherà l'applicazione del diritto alla riservatezza e di quello alla protezione dei dati personali, di cui agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione, nonché del diritto all'identità personale²¹. Pur in assenza di una casistica consolidata, un elemento sembra emergere evidente dalla lettura della decisione della Corte di giustizia: l'istante non è tenuto ad accompagnare la propria richiesta con approfondite argomentazioni, giuridiche o fattuali, inerenti la necessità di rimozione di quel dato risultato. Come osservato, l'accoglimento dell'istanza prescinde completamente da possibili pregiudizi collegati alla permanenza *on-line*, associato al proprio nome, del *link* in contestazione.

Anzi, la modulistica diffusa in Rete, allo stato, impone all'interessato esclusivamente due oneri di argomentazione rispetto alla propria istanza: il motivo per cui la pagina *web* cui rimanda il *link* da rimuovere lo riguarda e le ragioni per cui il relativo inserimento nei risultati di ricerca risulterebbe irrilevante, obsoleto o comunque discutibile²².

teoria, ove la richiesta di rimozione riguardi pagine contenenti immagini che ritraggono l'interessato, potrebbe essere necessario che il documento contenga la foto dello stesso.

²¹ Il diritto all'identità personale ha ad oggetto l'identità morale dell'individuo e deve essere inteso quale interesse della persona a non vedere alterata la verità della propria vita e delle proprie idee. Tale diritto va distinto da quello all'integrità morale, poiché prescinde dalla natura ingiuriosa o diffamatoria della notizia divulgata, ma ha come riferimento immediato semplicemente la verità dell'immagine complessiva del soggetto. Nel contesto della dottrina italiana, si vedano gli studi di A.DE CUPIS, *I diritti della personalità*, in *Trattato di diritto civile e commerciale*, diretto da CICU e MESSINEO, Milano, 1959, pp. 399 ss.; V.ZENO-ZENCOVICH, voce *Identità personale*, in *Dig. disc. priv.*, sez. civ., IX, Torino, 1993, pp. 294 ss.; F.MACIOCE, *Tutela civile della persona e identità personale*, Padova, 1984, *passim*; G.BAVETTA, voce *Identità (diritto alla)*, in *Enc. dir.*, XIX, pp. 953 ss.; G.ALPA – L.BONESCHI – M.BESSONE (a cura di), *Il diritto all'identità personale*, Padova, 1981, *passim*. Di recente, G.RESTA, *Identità personale ed identità digitale*, cit., cui si rinvia anche per gli ampi riferimenti di bibliografia. Cfr. anche M.L.RUFFINI GANDOLFI, *Mass media e tutela dell'identità personale. Il problema nel diritto statunitense*, Milano, 1987, *passim*.

²² Quella riportata nel testo è la formulazione tratta dal modulo *on-line* predisposto da Google. La sentenza della Corte di giustizia si esprime, invece, in questi termini: «*tale situazione si configura in particolare nel caso in cui i dati risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso. Pertanto, nell'ipotesi in cui si constati, in seguito a una domanda della persona interessata ai sensi dell'articolo 12, lettera b), della direttiva 95/46, che l'inclusione nell'elenco di risultati - che appare a seguito di una ricerca effettuata a partire dal suo nome - dei link verso pagine web, legittimamente pubblicate da terzi e contenenti informazioni veritiere relative alla sua persona, è, allo stato attuale, incompatibile con il citato articolo 6, paragrafo 1, let-*

Dunque, anche per la lettura estremamente – se non eccessivamente – lata offerta dalla Corte di giustizia dei termini del diritto dell'interessato, affidati quasi all'arbitrario volere dello stesso vista la genericità dei presupposti di valutazione (quali, ad esempio, la sopravvenuta carenza di pertinenza o di adeguatezza del dato presente *on-line*), il contenuto argomentativo dell'istanza di rimozione si può ridurre a pochissime sintetiche battute. Se le ragioni del richiedente possono, pertanto, essere affidate ad elementi giustificativi minimi, allo stato, per come configurato dalla Corte di giustizia, non pare esservi analoga considerazione per eventuali controinteressati (diversi dal gestore del motore di ricerca); la partecipazione al procedimento di potenziali soggetti aventi un interesse contrapposto a quello dell'interessato non è neppure adombrata nella decisione ed, anzi, in forza delle prassi adottate dai gestori dei motori di ricerca, risulta meramente eventuale.

In effetti, nel corpo della sentenza, si fa menzione della prospettiva del *service provider*, ritenuto portatore di un proprio diritto alla libertà d'impresa (anche *ex art. 17* della Carta dei diritti fondamentali dell'Unione), ma molto più vaga, se non inconsistente è l'attenzione per la platea (non necessariamente indistinta) degli utenti della Rete, che pure possono vantare un diritto al libero accesso alle informazioni comunque presenti nel *web*²³. Rispetto a questo specifico frangente, la decisione in commento

tere da c) a e), a motivo del fatto che tali informazioni appaiono, alla luce dell'insieme delle circostanze caratterizzanti il caso di specie, inadeguate, non pertinenti o non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento in questione realizzato dal gestore del motore di ricerca, le informazioni e i link in parola di cui al suddetto elenco di risultati devono essere cancellati motivo del fatto che tali informazioni appaiono, alla luce dell'insieme delle circostanze caratterizzanti il caso di specie, inadeguate, non pertinenti o non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento in questione realizzato dal gestore del motore di ricerca» (paragrafi 93-94).

²³ Da tempo gli studiosi si interrogano sui confini del diritto ad essere informati: vedi V.ZENO-ZENCOVICH, *Il controllo sulle metodologie informative*, in *Dir. Inf.* 1991, pp. 553 ss., e P.STANZIONE, *Informazione: potere, contropotere e le libertà del cittadino?*, in ID., *Diritto privato. Casi e problemi*, Salerno, 1992, pp. 339 ss. La letteratura in materia è, in ogni caso, particolarmente corposa: si rimanda, *inter alios*, a S.FOIS, *Principi costituzionali e libera manifestazione del pensiero*, Milano, 1957, *passim*; L.PALADIN, *Problemi e vicende della libertà d'informazione nell'ordinamento giuridico italiano*, in ID. (a cura di), *La libertà d'informazione*, Torino, 1979, pp. 33 ss.; V.CRISAFULLI, *Problematica della « libertà d'informazione »*, in *Il Politico*, 1964, pp. 284 ss.; A.M.SANDULLI, *La libertà d'informazione*, in *Problemi giuridici dell'informazione. Atti del XXVIII Convegno nazionale*, in *Quadrimestre*, Milano, 1979, pp. 15 ss.; A.LOIODICE, *Contributo allo studio sulla libertà di informazione*, Napoli, 1969, *passim*; M.MAZZIOTTI DI CELSO, *Appunti sulla libertà di manifestazione del pensiero nell'ordinamento italiano*, in *Scritti in onore di V. Crisafulli*, Padova, 1985, II, pp. 524 ss. In prospettiva comparatistica, cfr. A.BALDASSARRE, *Libertà*

pare gravemente deficitaria, nella misura in cui offre una visione profondamente restrittiva dell'art. 11 della Carta dei diritti fondamentali, stante l'evidente compromissione del diritto alla libertà di espressione, inteso in senso lato, che il procedimento in questione prefigura. La fondamentale prerogativa libertaria insita nell'accesso alle informazioni tramite Internet parrebbe, difatti, considerata (quasi sempre) soccombente rispetto al diritto a vedere protetta la propria riservatezza nell'ambito delle ricerche in rete, con un residuale rilievo esclusivamente nei termini di un trattamento svolto per finalità giornalistica²⁴. Il principale (se non unico) limite al diritto dell'interessato prospettato dalla Corte di giustizia è l'interesse pubblico all'accesso alla notizia, inteso come esplicitazione del diritto alla libertà d'informazione, con la sola (ed esemplificativa) menzione della notorietà del soggetto cui i dati personali sono riferiti. Eppure, nonostante esperienze analoghe, proprie del *web*, ove il rispetto del contraddittorio costituisce uno dei valori fondanti la legittimità stessa del procedimento²⁵, il soggetto portatore di tale interesse (non necessariamente superindividuale) non è né identificato, né chiamato a partecipare alla procedura di oscuramento del risultato di ricerca.

Siffatto interesse, come visto, non coincide certamente con quello del gestore del motore di ricerca e, per larghi tratti, può ritenersi pure distinto da quello del titolare del sito sorgente (la cui partecipazione al procedimento di deindicizzazione rimane comunque anch'essa puramente eventuale).

In realtà, è probabilmente qui che si può identificare il momento di maggiore criticità dell'impianto procedimentale immaginato dalla Corte di giustizia: il rischio di compromissione della libertà d'espressione avrebbe dovuto suggerire la prefigurazione di un meccanismo di partecipazione immediato e necessario quantomeno della competente Autorità amministrativa, che ben avrebbe potuto svolgere un compito di mediazione tra i

di stampa e diritto all'informazione nelle democrazie contemporanee (con particolare riguardo a Francia, RFT e USA), in *Pol. dir.*, 1986, pp. 586 ss.; J.RIVERO, *Il regime giuridico dell'informazione in Francia*, in L.PALADIN (a cura di), *La libertà d'informazione*, cit., pp. 65 ss.; M.D.FORKOSCH, *La libertà d'informazione negli Stati Uniti d'America*, *ivi*, pp. 195 ss.

²⁴ Cfr. CGE, Grande sez., 13 maggio 2014, causa C-131/12, cit., par. 85: «*inoltre, il trattamento da parte dell'editore di una pagina web, consistente nella pubblicazione di informazioni relative a una persona fisica, può, eventualmente, essere effettuato « esclusivamente a scopi giornalistici » e beneficiare così, a norma dell'articolo 9 della direttiva 95/46, di deroghe alle prescrizioni dettate da quest'ultima, mentre non sembra integrare tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca.*».

²⁵ Il riferimento è, innanzitutto, alle procedure di *notice and take down* sperimentate in materia di tutela della proprietà intellettuale, sulle quali si tornerà *infra*.

differenti interessi in conflitto. Al contrario, allo stato, l'Autorità amministrativa (o eventualmente quella giudiziaria) viene relegata a referente 'di secondo livello', nelle ipotesi di mancato accoglimento dell'istanza da parte del motore di ricerca. Ne risulta palese un quadro, invero dalla tinte piuttosto fosche, ove un numero enorme di istanze sarà vagliato ed accolto sulla base della sola valutazione (parziale) dell'interessato e del gestore del motore di ricerca, senza che vi sia stato un reale contraddittorio rispetto al possibile *vulnus* della libertà d'espressione.

5. Il ruolo 'ibrido' del gestore del motore di ricerca

Nel procedimento di deindicizzazione di un risultato dalle SERP, nell'impianto prefigurato dalla Corte di giustizia, un ruolo di centralità assoluta è indubbiamente affidato al gestore del motore di ricerca, chiamato ad operare, prima ancora (o, meglio, al posto) di qualsivoglia autorità di matrice pubblicistica, il *balancing* tra il diritto invocato dall'istante ed il configgente diritto alla conoscenza degli utenti della Rete, soddisfatto dalla immediata accessibilità della pagina sorgente in contestazione²⁶. Siffatta centralità discende direttamente dal passaggio decisivo della decisione in commento che identifica nel *service provider*²⁷ il responsabile del trattamento dei dati rappresentati dalle pagine indicizzate e, poi, rese disponibili, al momento della ricerca, in favore dell'utente. Secondo la Corte di giustizia, siamo dinanzi ad un trattamento distinto e separato rispetto a quello posto in essere dalle pagine sorgente, cioè quelle ove è materialmente caricata l'informazione che l'interessato vuol rendere irraggiungibile tramite il motore di ricerca.

D'altronde, si è visto come l'istanza di oscuramento ipotizzata dalla Corte non abbia ad oggetto la rimozione dell'informazione dalla Rete, bensì la semplice limitazione della accessibilità alla stessa, restringendone la possibilità di visualizzazione tramite un dato motore di ricerca ed a fronte di una ricerca basata sul nome dell'interessato.

Non a caso si discorre di diritto alla deindicizzazione, piuttosto che di

²⁶ Cfr. anche B.VAN DER SLOOT – F.J.ZUIDERVEEN BORGESIJUS, *Google and Personal Data Protection*, in A.LOPEZ-TARRUELLA (ed.), *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, Springer, 2012, pp. 75 ss.

²⁷ Nel caso specifico, il più importante, cioè Google. In tema, si rinvia a Cfr. anche S.VAN LOON, *The Power of Google: First Mover Advantage or Abuse of a Dominant Position?*, in A.LOPEZ-TARRUELLA (ed.), *Google and the Law*, cit., pp. 9 ss.

diritto alla cancellazione dell'informazione.

Dunque, il soggetto al centro del procedimento di rimozione, chiamato a valutare l'istanza ed a porre in essere l'operazione di oscuramento, non può che essere il responsabile del trattamento, cioè il motore di ricerca. Quello del gestore del motore di ricerca nel procedimento di rimozione è un ruolo decisamente problematico, dal momento che, per un verso, non si può ragionevolmente immaginare che un operatore di mercato muti la propria natura a fronte delle istanze degli utenti, ma, per un altro, l'impianto procedurale delineato dalla Corte di giustizia si fonda tutto, almeno in prima istanza, sulla delega al privato del giudizio di temperamento tra diritti di rango costituzionale. In altre parole, nel compito affidato al gestore del motore di ricerca dalla Corte di giustizia pare di poter scorgere un tentativo (tutto teorico, invero) di 'ibridarne' la natura: in astratto, questi dovrebbe ergersi a sorta di paladino della libertà di accesso all'informazione in Rete, rigettando l'istanza dell'interessato nell'ottica della tutela di un interesse collettivo alla conoscenza ed anche contro il proprio interesse d'impresa (che dovrebbe ragionevolmente indurre alla opposta soluzione del generalizzato accoglimento delle istanze con minimizzazione dei costi di procedura come dei rischi di sanzioni e di richieste risarcitorie)²⁸.

In realtà, come accennato, una aspettativa di questo tipo è assolutamente illusoria: non si può pretendere da un operatore di mercato privato di anteporre al proprio interesse d'impresa quello della collettività alla conoscenza, soprattutto allorquando ciò possa comportare esternalità negative non preventivabili o difficilmente sostenibili. Al più, l'operatore privato potrebbe perseguire l'interesse collettivo in forma indiretta, nel caso in cui quest'ultimo coincida con il proprio interesse individuale: nella fattispecie in esame, ciò potrebbe verificarsi ove mai, ad esempio, un numero particolarmente elevato di istanze, tutte massicciamente accolte, potrebbe finire per minare l'affidabilità stessa del motore di ricerca con perdita di appeal di mercato²⁹. Eppure, proprio al fine di evitare distorsioni di questo tipo, anche in coerenza con principi precedentemente espressi dalla Corte di giustizia³⁰, sarebbe stato auspicabile affidare il vaglio delle

²⁸ In tema, M. THOMPSON, *In Search of Alterity: On Google, Neutrality and Otherness*, in A. LOPEZ-TARRUELLA (ed.), *Google and the Law*, cit., pp. 355 ss.

²⁹ Vedi R. PARDOLESI, «Goooooglelaw». *Del ricorso alla disciplina antitrust per colpire il tiranno benevolente*, in *Foro it.*, 2013, V, pp. 18 ss.

³⁰ Si pensi, in tal senso, ai principi sanciti, quasi nei medesimi giorni, da CGE, Grande sez., 8 aprile 2014, nelle cause riunite C-293/12 e C-594/12, in *Dir. Inf.* 2014, p. 851. Cfr. anche CGE, 24 novembre 2011, cause riunite C-468/10 e C-469/10, in *Foro it.*,

istanze di deindicizzazione direttamente ai Garanti nazionali oppure prevederne l'interpello necessario da parte dei motori di ricerca: ciò avrebbe consentito un'indubbia garanzia di obiettività di giudizio, con effettivo contemperamento degli interessi in contrapposizione. Ad ogni modo, nel modello di procedimento ipotizzato dalla Corte di giustizia, l'attività che il motore di ricerca è chiamato, in concreto, a porre in essere, in virtù delle prerogative incombenti sullo stesso quale titolare del trattamento, possono distinguersi in due momenti: valutazione dell'istanza e, poi, eventuale oscuramento. La prima fase è certamente quella più delicata³¹, allorché il gestore del motore di ricerca è chiamato al vaglio della richiesta di oscuramento proposta dall'interessato. Secondo il modello attualmente diffuso dai principali operatori di mercato, l'interessato, dunque, ha accesso, attraverso un link dalla schermata iniziale di ricerca, ad un apposito modulo precompilato nel quale è necessario indicare: a) la normativa nazionale di riferimento; b) il nome che ha condotto alla visualizzazione di uno o più risultati oggetto di istanza; c) il nome anagrafico completo del richiedente; d) un indirizzo di posta elettronica; e) l'URL dei risultati che si desidera vengano rimossi; f) una sintetica motivazione; g) la copia di un documento d'identità; h) la dichiarazione di esattezza e conformità delle dichiarazioni e delle informazioni riportate; i) firma e data. Una volta inoltrato il modulo on-line, il gestore del motore di ricerca si riserva di valutare la richiesta, effettuando il segnalato bilanciamento tra il diritto alla *privacy* della persona e «il diritto di rendere accessibili le informazioni e l'interesse pubblico a trovarle». Secondo le sintetiche spiegazioni fornite dai prestatori che hanno adottato procedure di questo tipo, l'istanza verrà valutata tenendo in debita considerazione la circostanza che i risultati contengano informazioni obsolete e il fatto che le informazioni siano di interesse pubblico: una volta esperita la fase di valutazione, i risultati verranno poi rimossi o mantenuti visualizzabili all'atto di una ricerca. La seconda attività che il motore di ricerca è chiamato a compiere, qualora l'istanza presentata sia meritevole di accoglimento, è di natura strettamen-

2012, IV, pp. 1 ss., con nota di PALMIERI, *Tutela dei dati personali e interesse alla circolazione delle informazioni: ancora un monito della Corte di giustizia sul rispetto degli equilibri faticosamente intrecciati*.

³¹ In effetti, all'indomani della decisione, in forza della previsione della responsabilità del gestore del motore di ricerca quale titolare del trattamento è disceso l'immediato obbligo positivo di uniformarsi ai precetti fissati dalla Corte, con elaborazione di un sistema di notifica e rimozione dei collegamenti alle pagine indicizzate contenenti dati personali ritenuti non conformi dagli interessati. Il primo motore di ricerca ad introdurre una modulistica *ad hoc*, in costante evoluzione, è stato Google; di recente, analoga procedura è stata adottata anche da Bing.

te tecnica e consiste nell'oscuramento dello specifico risultato di ricerca da quelli associati al nome dell'utente, segnalato da quest'ultimo tramite l'indicazione del corrispondente URL³².

In ultima analisi, con la previsione di una responsabilità diretta dei gestori dei motori di ricerca per i dati personali 'intercettati' nel web e la conseguente introduzione di una procedura di 'dialogo diretto' tra interessato e gestore, la decisione finisce per obbligare i providers a modificare – quantomeno per lo spazio giuridico comunitario – le policies di gestione dei propri servizi con precipuo riferimento all'accoglimento ed al vaglio delle istanze di oscuramento, approntando uno specifico canale di intervento in favore degli utenti. Si tratta di un procedimento di interlocuzione diretta tra gestore del servizio di ricerca ed interessato che si contraddistingue, per autonomia ed indipendenza, rispetto alle procedure esperibili innanzi ai Garanti della *privacy* nazionali e, ancora, al ricorso alla 'tradizionale' tutela giurisdizionale dei diritti. Chiaramente, la linea di demarcazione rispetto agli interlocutori istituzionali cui l'interessato può rivolgere la propria istanza in seconda battuta è segnata anche e soprattutto dalla natura privatistica che caratterizza il gestore del motore di ricerca, che non può essere confuso con una sorta di 'paladino' del diritto alla conoscenza nel web. Questi, infatti, nella identificazione del point of balance tra diritto alla riservatezza e quello alla conoscenza di una data informazione presente in Rete non sarà animato dalla prospettiva del migliore equilibrio tra posizioni individuali (e/o superindividuali) in un dato contesto sociale, secondo una sorta di logica (para)pubblicistica e con surrettizio riconoscimento allo stesso di funzioni quasi costituzionali³³. Al contrario, sebbene la decisione della Corte di giustizia taccia completamente sul punto, sarebbe ingenuo – rectius, illogico – attendersi che il gestore del motore di ricerca sia mosso, nel vagliare le istanze proposte dai consociati, da una finalità diversa da quella di impresa: siffatta prospettiva, che non può non animare qualsivoglia operatore di mercato, nella maggior parte dei contesti economici, indica come obiettivo primario, innanzitutto, la minimizzazione del rischio. Ebbene, visto che la rimozione dell'informa-

³² Da segnalare che, di recente, in calce alle ricerche che siano state interessate da procedimenti di rimozione, Google ha cominciato a pubblicare un *warning*, del seguente tenore letterale: «*Alcuni risultati possono essere stati rimossi nell'ambito della normativa europea in sulla protezione dei dati*».

³³ Analoghe perplessità sono state espresse, all'indomani della decisione, da O.POLLICINO, *Google rischia di « vestire » un ruolo para-costituzionale*, in *Il Sole24 Ore*, 15 maggio 2014, 45, nonché da A.PALMIERI - R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete*, cit., pp. 3 ss.

zione dai risultati di ricerca soltanto raramente può avere controinteressati qualificati, l'opzione nella direzione della minimizzazione del rischio d'impresa, nel caso di specie, si identifica nell'evitare possibili aggravii connessi ad istanze risarcitorie di interessati la cui richiesta di rimozione sia stata disattesa e/o a sanzioni imposte dalle Autorità Garanti nazionali. In ultima analisi, allora, un operatore di mercato, a fronte di un'istanza proposta da un cittadino comunitario, gravato del 'dilemma' tra accoglimento o rigetto della domanda presentata, non potrà che propendere pressoché sempre per l'accoglimento delle richieste di deindicizzazione, in quanto scelta economicamente più efficiente in termini di riduzione di potenziali output negativi conseguenti.

6. Il procedimento 'notice and take down' del DMCA. Un modello possibile?

Secondo l'impostazione propria della sentenza in commento, la prima (e, nella maggior parte delle occasioni, esclusiva) comparazione tra interesse del singolo utente e quello, di carattere pubblicistico, alla conoscenza viene rimessa ad un soggetto privato, cioè il gestore del motore di ricerca. Ora, l'affidamento di funzioni di vigilanza e controllo sui contenuti del *web* a soggetti privati qualificati – come i motori di ricerca, appunto – rappresenta, già da diversi anni, una importante realtà rimediale ad applicazione globale, soprattutto allorché accompagnata—ove disattesa—dallo 'spettro' di potenziali conseguenze risarcitorie in prospettiva di *private enforcement*. In particolare, da un punto di vista procedimentale, il riferimento immediato non può che essere l'esperienza della tutela dei diritti di proprietà intellettuale nell'ambito del *web*³⁴, ove le procedure di *notice and take down*, quale è quella disegnata oggi in materia dalla Corte di giustizia, sono state introdotte per la prima volta, già nel 1998, dal legislatore statunitense nel contesto della tutela del diritto d'autore *on-line*, con l'entrata in vigore del *Digital Millenium Copyright Act* (DMCA)³⁵. Si tratta di una procedura

³⁴ Sulla diversa tutela riservata nella rete ai diritti della personalità rispetto a pretese di tipo proprietario si rimanda a quanto scritto, di recente, da G.RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. Inf.* 2014, pp. 196 ss.

³⁵ Sul tema v. A.C.YEN, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability and the First Amendment*, in 88 *Georgetown L.J.*, 2000, pp. 1833 ss.; G.LICHTMAN – E.POSNER, *Holding Internet Service Providers Accountable*, in *John M. Olin & Economics working paper*, no. 217, Chicago, 2004; K.TAYPALE, *Secondary Liability on the Internet: Towards a Performative Standard for Constitutive*

articolata, caratterizzata da tempi contingentati e dall'intervento di diverse figure, ove tuttavia è centrale e costantemente perseguita, in ogni fase, la garanzia del contraddittorio tra le diverse parti interessate al contenuto informativo presente in Rete ed oggetto di contestazione. Nello specifico, secondo il meccanismo procedimentale previsto dal modello statunitense, in forza del disposto della sec. 512, (c) (2), 17 U.S.C., per andare esente da responsabilità per eventuali violazioni del *copyright*, il *provider* deve, innanzitutto, nominare un soggetto addetto alla ricezione dei reclami dei titolari di diritti d'autore (c.d. *designated agent*), identificabile con facilità dal pubblico per mezzo di appositi *link* inseriti e ben visibili sulla *homepage* delle piattaforme³⁶. La *notification* consiste in una comunicazione scritta inviata al *designated agent*, che deve contenere elementi in buona parte analoghi a quelli propri del modello di segnalazione diffuso da Google per la deindicizzazione delle pagine *web*: *a*) la firma (autografa o elettronica) del soggetto interessato o del legale rappresentante; *b*) l'indicazione dell'opera protetta che si reputa essere stata abusivamente utilizzata; *c*) la specificazione dell'URL che favorisca la corretta collocazione dei materiali lesivi; *d*) le informazioni ragionevolmente sufficienti sull'identità del presunto autore della violazione, che consentano al *provider* di contattarlo; *e*) un'espressa dichiarazione in cui il ricorrente afferma di agire in buona fede a tutela dei propri diritti; *f*) un'ulteriore dichiarazione che comprovi l'accuratezza delle informazioni fornite, nonché la legittimazione ad agire avverso le condotte oggetto del reclamo³⁷. La sec. 512 (g) prevede, poi,

Responsibility, CAS Working Paper Series, 4, 2003. Nella dottrina italiana, si rinvia anche a L.NIVARRA, voce *Responsabilità del provider*, in *Dig. disc. priv.*, Torino, 2003, pp. 1195 ss.; M.FRANZONI, *La responsabilità del provider*, in *Resp. com. impr.*, 1997, pp. 767 ss., e G.M.RICCIO, *La responsabilità civile degli internet providers*, Torino, 2002, *passim*.

³⁶ Le generalità dei *designated agent*, preposti alla ricezione ed al vaglio delle notifiche di *infringement*, vengono poi trasmesse al *Register of Copyright*, organismo statale che mantiene liberamente accessibili sul *web* alcune pagine informative sulle procedure di rimozione. Per una ricostruzione della normativa statunitense e un confronto con le procedure amministrative a tutela del diritto d'autore *on-line* recentemente introdotte dall'Autorità garante per le comunicazioni (AGCOM), si rimanda all'indagine svolta da G.GIANNONE CODIGLIONE, *Illeciti su Internet e rimedi nel diritto d'autore* (Tesi di dottorato), Università di Salerno, 2014, spec. Pp. 99 ss. e pp. 158 ss.

³⁷ Una segnalazione priva di tali elementi non può costituire prova della effettiva conoscenza in capo al prestatore di servizi di eventuali violazioni e, pertanto, non rileverà ai fini dell'esenzione di cui alla sec. 512 (c) (1) (A). Nel caso di parziale incompletezza delle informazioni fornite – e quando esse sostanzialmente integrano i requisiti di cui alle precedenti lettere *b*), *c*) e *d*) – il prestatore viene considerato non a conoscenza della violazione soltanto ove abbia prontamente contatto l'autore della *notification*, invitandolo a rettificare il contenuto.

una generica presunzione di irresponsabilità a favore del *provider* che abbia, in buona fede, disabilitato l'accesso o rimosso contenuti ed attività sulla base di fatti o circostanze che ne comprovassero l'apparente illiceità, a prescindere dal fatto che, in seguito ad ulteriori accertamenti, l'apparenza abbia trovato conferma oppure no. Questa presunzione non trova applicazione, però, nei casi in cui il prestatore non garantisca un contraddittorio minimo tra il titolare del *copyright* che si presume violato e l'autore delle attività o dei contenuti oggetto di notifica: ne deriva la necessità di avvertire repentinamente il destinatario della misura restrittiva dell'avvenuta rimozione, ponendolo così in condizione di produrre una contronotifica (c.d. *counter notification*). La contronotifica consiste in una dichiarazione in forma scritta in cui, indicata la precisa localizzazione fisica del contenuto (consistente quasi sempre nell'URL), se ne contesta l'avvenuta rimozione o la disabilitazione dell'accesso. Inoltre, il *subscriber* è tenuto a dichiarare – pena la condanna per falsa testimonianza ('*perjury*') – di avere buoni motivi per credere («*a good faith belief*») che i contenuti siano stati oggetto di una rimozione a causa di un errore o di una non corretta identificazione. Il firmatario di una *counter notification*, infine, deve sottoscrivere un'apposita clausola in cui dichiara di rimettersi alla giurisdizione della competente *Federal District Court*, accettando contestualmente che l'*agent* provveda ad inviare il contenuto della contronotifica alla controparte/*claimant*. Ricevuta la *counter notification*, l'*agent* deve infatti darne immediata comunicazione all'autore della segnalazione, informandolo che provvederà entro dieci giorni alla rimessione in pristino dei contenuti precedentemente rimossi³⁸. Al fine di prevenire eventuali rischi di *chilling effects* connessi al potenziale abuso ed alla strumentalizzazione di questo articolato sistema di rimozione su istanza di parte, che pure affida al *provider* il potere di agire direttamente sui contenuti, garantendo altresì un contraddittorio minimo, è stata elaborata una specifica ipotesi di responsabilità per *misrepresentation*. La *subsection* (f) dispone che chiunque fornisca intenzionalmente notifiche false, erronee o, ancora, riferite a materiali o attività poi rimossi o disabilitati erroneamente o a seguito di una segnalazione non corretta, può essere chiamato a rispondere di tutti i danni eventualmente cagionati con la propria condotta tanto al *subscriber*, quanto al *provider*, oltre che essere condannato al pagamento delle spese

³⁸ Il ripristino dello *status quo ante* può essere attuato dal prestatore dopo non meno di dieci e non più di quattordici giorni lavorativi dalla ricezione della contro-notifica, eccetto nei casi in cui l'*agent* stesso riceva dal *claimant* la comunicazione dell'introduzione di un'azione legale volta ad ottenere la cessazione dei comportamenti reputati illeciti rispetto ai materiali oggetto di notifica.

processuali e legali.

Dunque, il descritto modello di procedimento di rimozione/ oscuramento di contenuti illeciti presenti in Rete indica alcuni elementi fondanti che dovrebbero caratterizzare qualsivoglia intervento analogo, soprattutto allorché affidato ‘in gestione’ – quantomeno in prima battuta – direttamente al *provider*. Il primo punto focale è certamente quello della ricerca di garanzia costante del contraddittorio tra tutte le parti interessate al contenuto *on-line* oggetto di contestazione: da questo punto di vista, nella procedura del DMCA, il prestatore di servizi è costantemente chiamato a favorire ed a mediare una sorta di colloquio tra gli interessi in contrapposizione (tramite il meccanismo della *notification* e della *counter notification*). Il rispetto del contraddittorio, per il *provider*, non rappresenta tuttavia un mero obiettivo ideale e teorico, bensì un risultato concreto da perseguire in qualsivoglia procedimento, visto che il rischio è quello di essere chiamato, in mancanza, a rispondere dei danni conseguenti a rimozioni arbitrarie.

Questo profilo, ad oggi, risulta completamente trascurato nell’*iter* procedimentale immaginato dalla Corte di giustizia per la deindicizzazione dei risultati di ricerca, soprattutto ove si pensi che, addirittura, la stessa partecipazione alla procedura del titolare del sito sorgente, da rimuovere dai risultati di ricerca, è meramente eventuale, sicché lo stesso potrebbe venire a conoscenza soltanto dopo molto tempo (o, addirittura, mai) dell’avvenuto oscuramento della propria pagina. Un ulteriore elemento caratterizzante il sistema di *notice and take down* del DMCA è la marcata responsabilizzazione degli utenti che interagiscono con il *provider* nel corso del procedimento: il rischio di censura di contenuti lecitamente presenti in Rete e di abuso dello strumento è minimizzato attraverso strumenti forti di *deterrence* direttamente incombenti tanto sul firmatario della richiesta di oscuramento, quanto su colui che alla stessa si oppone. Entrambi i soggetti, come visto, all’atto della presentazione della *notification* o della *counter notification* sono resi edotti dell’assunzione di specifiche responsabilità, anche di matrice risarcitoria, collegate a dichiarazioni mendaci o inesatte rese nella richiesta di intervento formulata oppure al tentativo di abuso realizzato tramite la stessa. Seppure comunque riconducibile alle regole generali in materia di illecito aquiliano, una specifica assunzione di responsabilità, in ipotesi di abuso del diritto, sottoscritta dall’interessato al momento della presentazione del modulo di richiesta di rimozione di un *link* presente nelle SERP potrebbe rappresentare un forte strumento di dissuasione rispetto ad istanze pretestuose oppure dolosamente preordinate a cagionare danni ad altri utenti del *web* o, magari, allo stesso gestore del

motore di ricerca. Infine, devono pure segnalarsi, quali ulteriori peculiarità positive della procedura introdotta negli Stati Uniti a tutela del *copyright on-line*, l'esistenza di meccanismi formalizzati di coordinamento tra la fase di controllo di matrice privatistica e quella, pubblicistica, affidata ad organi statali, nonché la previsione di una tempistica certa e ben circoscritta ai fini dell'assunzione di una decisione da parte del *provider* circa le sorti del contenuto informativo contestato. Se il procedimento di *notice and take down* statunitense sembra, allora, porsi quale modello particolarmente evoluto nel contesto di analoghe procedure, aventi carattere innanzitutto privatistico, inerenti la rimozione di contenuti presenti sul *web*, va pure detto che tale articolato schema di procedimento non trova un omologo nella disciplina comunitaria in materia di commercio elettronico. La direttiva 2000/31/CE, frutto di un chiaro (ma decisamente incompleto) esercizio di riproduzione da parte del legislatore comunitario, si limita difatti a prevedere, ai considerando 40 e 46, l'auspicio dell'introduzione di sistemi «*rapidi ed affidabili, che siano idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime*», puntualizzando altresì che il prestatore, per godere di una limitazione di responsabilità, deve agire immediatamente per rimuovere le informazioni o per disabilitare l'accesso «*appena sia informato o si renda conto delle attività illecite*», nel rispetto del principio della libertà d'espressione³⁹. Per quanto riguarda lo specifico ambito della tutela della riservatezza e della protezione dei dati personali, queste indicazioni, che fanno riferimento alla diffusione di informazioni illecite nell'ambito delle regole di responsabilità civile dell'*internet service provider*, andrebbero poi poste in correlazione con le statuizioni proprie della direttiva 95/46/CE, che – come visto – pure identifica in favore dell'interessato una serie di poteri, quali quelli di rettifica, adeguamento, cancellazione dei

³⁹ Si rinvia, sul tema, a S.SICA, *Recepita la direttiva sul commercio elettronico: commento al d.lgs. 70/03*, in *Corr. giur.*, 2003, 9, pp. 1225-1247; ID., *Le responsabilità civili*, in E.TOSI (a cura di), *Commercio elettronico e servizi della società dell'informazione*, Milano, 2003, pp. 127 ss.; P.STANZIONE – S. SICA, *Commercio elettronico e categorie civilistiche*, Milano, 2002, *passim*, e S.SICA – N.BRUTTI, *Internet e commercio elettronico: la responsabilità civile*, in V.D'ANTONIO – S.VIGLIAR (a cura di), *Studi di diritto della comunicazione. Persone, società e tecnologie dell'informazione*, Padova, 2009, pp. 121-152. Cfr. anche G.M.RICCIO, *La responsabilità civile degli internet providers*, cit.; ID., *La responsabilità civile degli internet providers nel d.lgs. n. 70/2003*, in *Danno e resp.*, 2003, pp. 1158 ss.; G.CASSANO – I.P.CIMINO, *Il nuovo regime di responsabilità dei providers: verso la creazione di un novello « censore telematico »? Un primo commento agli artt. 14-17 del d. lgs. n. 70/1003*, in *Giur. it.*, 2004, pp. 671 ss.; E.SANNA, *Il regime di responsabilità dei providers intermediari di servizi della società dell'informazione*, in *Resp. civ. prev.*, 2004, I, pp. 279 ss.; O.TROIANO, *L'impresa di content, host ed access providing*, in *AIDA*, XVI, Milano, 2008.

propri dati personali, nonché di opposizione al trattamento in determinate circostanze. Tuttavia, la direttiva del 2000 (così come anche quella del 1995) non regolamentano una disciplina generale in merito alle procedure di intervento del prestatore a fronte di istanze dei privati, né tracciano dei criteri guida per l'espletamento delle stesse, limitandosi ad incoraggiarne una possibile futura introduzione, nel generale auspicio che il tutto possa avvenire a seguito di un preventivo dialogo tra tutte le parti interessate⁴⁰.

Ne consegue che quando, come nel caso in esame, il formante giurisprudenziale impone il ricorso a siffatte procedure, il privato finisce per essere investito non soltanto, in prospettiva sostanziale, del bilanciamento tra prerogative contrapposte degli utenti della Rete, bensì anche, in ottica formale, della definizione delle modalità di esplicazione del relativo procedimento (e la forma, non di rado, sopravanza e condiziona la sostanza)⁴¹.

7. L'ordinamento italiano e l'orientamento di Cass. n. 5525/2012

Per quanto riguarda lo specifico dell'ordinamento italiano, la prospettiva fatta propria dalla Corte di giustizia si rivela, invero, differente rispetto a quella proposta dalla Corte di Cassazione, allorché è stata chiamata a decidere una fattispecie analoga⁴². Anche da un punto di vista procedimentale, la Corte di giustizia finisce per delineare un doppio canale di trattamento dei dati sul web. Da una parte, riconosce indirettamente la responsabilità del gestore dei siti che contengano informazioni e dati personali, con obbligo di curarne l'aggiornamento, la contestualizzazione

⁴⁰ Cfr. considerando 40, dir. 2000/31/CE.

⁴¹ In tema, DE BUSSE, *Privatization of Information and the Data Protection Reform*, in GUTWIRTH - LEENES - DE HERT (eds.), *Reloading Data Protection*, cit., pp. 129 ss.

⁴² Il riferimento completo è Cass., sez. III civ., 5 aprile 2012, n. 5525, in *Foro it.*, 2013, I, pp. 305 ss., con nota di E.TUCCI; in *Dir. Inf.* 2012, pp. 383 ss., con note di G.FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, e di T.E.FROSINI, *Il diritto all'oblio e la libertà informatica*; in *Danno e resp.*, 2012, pp. 747 ss., con nota di F.DI CIOMMO - R. PARDOLESI, *Trattamento dei dati personali e archivi storici accessibili in Internet: notizia vera, difetto di attualità, diritto all'oblio*; in *Corr. giur.*, 2012, pp. 769 ss., con nota di A.DI MAJO, *Il tempo siamo noi ...*; in *Nuova giur. civ.*, 2012, I, pp. 843 ss., con nota di A.MANTELERO, « *Right to be forgotten* » ed *archive storici dei giornali - La Cassazione travisa il diritto all'oblio*. Il precedente attiene alla controversia instauratasi tra un politico, arrestato per corruzione all'inizio degli anni '90 ma poi prosciolto, ed un quotidiano, nel cui archivio *on-line* era ancora liberamente accessibile la notizia dell'arresto, senza alcun contestuale riferimento al positivo epilogo della vicenda processuale.

ed, in determinati casi, la rimozione. Questo indirizzo è stato accolto, da tempo, dal Garante della *privacy* nazionale, che in numerose occasioni ha ordinato l'aggiornamento delle pagine contenute negli archivi on-line delle testate giornalistiche⁴³. D'altra parte, tuttavia, i medesimi dati, provenienti dai c.d. siti sorgente, allorquando sottoposti al processo di raccolta, catalogazione, indicizzazione e memorizzazione temporanea dal motore di ricerca, divengono oggetto di un trattamento 'diverso', poiché avente differenti finalità e modalità di espletamento. Come visto, su questo preciso aspetto, la pronuncia della Corte di giustizia segna una netta linea di demarcazione con gli orientamenti precedenti⁴⁴.

In effetti, se il Garante per la protezione dei dati personali italiano, già in alcuni provvedimenti, aveva riconosciuto l'autonomia del trattamento svolto dai motori di ricerca, sottolineando la diversa efficacia in termini di diffusione dei dati e di incidenza che la percezione degli stessi produce sugli utenti⁴⁵, la Suprema Corte, invece, ha sino ad oggi privilegiato un approccio più cauto sul tema, attribuendo rilevanza esclusiva al profilo di responsabilità gravante sul sito sorgente, nella prospettiva di una posizione non 'attiva' del motore di ricerca rispetto al controllo e alla conoscenza dei dati memorizzati anche temporaneamente⁴⁶. La Cassazione, in un'ot-

⁴³ Garante protezione dati personali, 24 gennaio 2013, doc. web n. 2286820; 8 aprile 2009, doc. web n. 1617673; 11/12/2008, doc. web n. 1583162, in www.garanteprivacy.it [consultato il 30/09/2014].

⁴⁴ V. CGE, Grande sez., 13 maggio 2014, causa C-131/12, *Google c. AEPD e Mario Costeja Gonzales*, in Appendice a questo Volume, punto 28.

⁴⁵ Cfr. Garante protezione dati personali, 18 gennaio 2006, doc. web n. 1242501, in www.garanteprivacy.it: «(...) presso il motore di ricerca in questione risulta effettuato un autonomo trattamento di dati personali della ricorrente, in particolare attraverso la creazione e la conservazione di cosiddette copie cache di pagine web pubblicate su siti 'sorgente'; (...) rispetto a tali tipologie di trattamento gli interessati possono formulare legittimamente richieste di esercizio dei propri diritti cui va dato riscontro senza ritardo, qualora il Codice sia applicabile» e ancora 19 dicembre 2008, in *Rep. Foro it.*, 2013, Merito extra, n. 2013.73.3: «(...) tali motivi di opposizione appaiono meritevoli di specifica tutela, tenuto conto delle peculiarità del funzionamento della rete Internet che può comportare la diffusione di un gran numero di dati personali riferiti a un medesimo interessato e relativi a vicende anche risalenti nel tempo – e dalle quali gli interessati stessi hanno cercato di allontanarsi, intraprendendo nuovi percorsi di vita personale e sociale – che però, per mezzo della rappresentazione istantanea e cumulativa derivante dai risultati delle ricerche operate mediante i motori di ricerca, rischiano di riverberare comunque per un tempo indeterminato i propri effetti sugli interessati come se fossero sempre attuali; ciò, tanto più considerando che il successivo utilizzo degli esiti delle ricerche effettuate sulla rete Internet mediante i motori di ricerca può avvenire per gli scopi più diversi e non sempre per finalità di ricerca storica in senso proprio».

⁴⁶ Cfr. Cass. n. 5525/2012, cit., ove si legge che «il titolare di un organo di informazione

tica sostanziale non dissimile da quella propria della Corte di giustizia, propone una ricostruzione dinamica della tutela della riservatezza, tesa ad esaltare la dimensione del controllo da parte degli interessati sull'utilizzo e sul destino dei propri dati, ponendo al centro del proprio *decisum* una netta affermazione del diritto all'oblio. In particolare, la Suprema Corte riconosce che se l'interesse pubblico sotteso al diritto all'informazione (ex art. 21 Cost.) costituisce un limite al diritto fondamentale alla riservatezza (di cui agli artt. 21 e 2 Cost.), «*al soggetto cui i dati pertengono è correlativamente attribuito il diritto all'oblio, e cioè a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino ormai dimenticate o ignote alla generalità dei consociati*»⁴⁷. L'impostazione muta radicalmente allorché la Cassazione italiana cala siffatto principio nel contesto della Rete, proponendo una lettura delle informazioni in essa presenti differente rispetto a quella della Corte di giustizia, fondata sulla distinzione tra archivio e memoria del *web*⁴⁸. Sulla base di siffatta partizione, poiché vengono ritenuti archivi soltanto quelli dei singoli utenti che accedono alla rete

è tenuto a garantire la contestualizzazione e l'aggiornamento della notizia di cronaca, successivamente spostata nell'archivio storico anche se pubblicato su internet, al fine di consentire alla medesima di mantenere i caratteri di verità ed esattezza e quindi di liceità e correttezza, a tutela del diritto dell'interessato al trattamento alla propria identità personale o morale nonché a salvaguardia del diritto del cittadino utente di ricevere un'informazione completa e corretta».

⁴⁷ Vedi anche Cass. 9 aprile 1998, n. 3679, in *Foro it.*, 1998, pp. 123 ss.

⁴⁸ V. Cass. n. 5525/2012, cit., secondo cui «*mentre l'archivio si caratterizza per essere ordinato secondo criteri determinati, con informazioni intercorrelate volte ad agevolarne l'accesso e a consentirne la consultazione, la rete internet costituisce in realtà un ente ove le informazioni non sono archiviate ma solo memorizzate. Esso è dotato di una memoria illimitata e senza tempo, emblematico essendo al riguardo il comune riferimento al 'mare di internet', all'oceano di memoria' in cui gli internauti 'navigano'. La memoria della rete internet non è un archivio, ma un deposito di archivi. Nella rete internet le informazioni non sono in realtà organizzate e strutturate, ma risultano isolate, poste tutte al medesimo livello ('appiattite'), senza una valutazione del relativo peso, e prive di contestualizzazione, prive di collegamento con altre informazioni pubblicate (come segnalato anche in dottrina, lo stesso pagerank indica quando una pagina è collegata da link, non a quali informazioni essa debba essere correlata, né fornisce alcun dato sulla qualità dell'informazione). Si pone allora l'esigenza di attribuzione della fonte dell'informazione ad un soggetto, della relativa affidabilità, della qualità e della correttezza dell'informazione. Al riguardo, a parte il rilievo che come osservato anche in dottrina sul piano pratico la pur possibile attività di cancellazione può essere ad esempio chiesta al motore di ricerca Google la rimozione di una pagina (Omissis) o di un intero URL (Omissis) non è comunemente posta in essere, non può invero nemmeno prescindere dalla considerazione della circostanza della sussistenza di siti che memorizzano i dati scomparsi da altri siti (come, ad es., (Omissis), il quale presta un servizio denominato Way back machine)».*

e quelli dei titolari dei siti, che costituiscono la fonte dell'informazione (c.d. siti sorgente), il motore di ricerca viene degradato a mero intermedio telematico, che offre un sistema automatico di reperimento di dati e informazioni attraverso parole chiave, un mero *database* che indicizza i testi sulla rete e offre agli utenti un accesso per la relativa consultazione. Dunque, la Suprema Corte italiana non ritiene di poter identificare un rapporto diretto tra gestore del motore di ricerca ed interessato, né conseguentemente si pone il problema della possibile sola deindicizzazione del risultato di ricerca (che tuttavia continua ad essere presente in Rete), ma imputa in via esclusiva e diretta al titolare della pagina sorgente il dovere di aggiornare e contestualizzare il dato (anche in considerazione di un'eventuale indicizzazione da parte del motore di ricerca⁴⁹).

Per certi versi, la decisione della Corte di giustizia potrebbe essere letta anche come una sorta di completamento del principio affermato dalla Cassazione italiana, allorché si consideri che dinanzi all'interessato potrebbero aprirsi due possibili scenari a fronte della obsolescenza dei dati personali presenti in rete che lo riguardano: invocare un intervento direttamente sulla sostanza dell'informazione oppure soltanto sulla reperibilità della stessa. Nel primo caso, evidentemente, l'istanza di aggiornamento e contestualizzazione dei dati e delle informazioni, precedentemente pubblicate come notizie di cronaca (o di altra natura), andrà proposta direttamente al titolare del sito sorgente; nel secondo caso, invece, dati ed informazioni resteranno invariati nella sostanza e l'istanza andrà proposta al motore di ricerca, affinché si limiti ad oscurare pagine sorgente inattuali. I presupposti fondativi di ambedue le possibilità di intervento sui propri dati personali sono i medesimi, tant'è che, non a caso, si è visto come la ricostruzione del diritto alla riservatezza ed alla protezione dei dati personali, così come quello inerente la protezione dell'identità personale proposta dalla Corte di giustizia sia sostanzialmente conforme a quella del precedente di Cassazione del 2012.

Ciò che muta, tuttavia, non è soltanto il destinatario dell'istanza

⁴⁹ Secondo Cass. n. 5525/2012, cit., infatti, «*in ipotesi, come nella specie, di trasferimento D.Lgs. n. 196 del 2003, ex art. 11, comma 1, lett. b), di notizia già di cronaca (nel caso, relativa a vicenda giudiziaria di personaggio politico) nel proprio archivio storico, il titolare dell'organo di informazione (nel caso, la società Rcs Quotidiani s.p.a.) che avvalendosi di un motore di ricerca (nel caso, Google) memorizza la medesima anche nella rete internet tenuto ad osservare i criteri di proporzionalità, necessità, pertinenza e non eccedenza dell'informazione, avuto riguardo alla finalità che ne consente il lecito trattamento, nonché a garantire la contestualizzazione e l'aggiornamento della notizia già di cronaca oggetto di informazione e di trattamento*».

(titolare della pagina sorgente o del motore di ricerca) e l'oggetto della stessa (aggiornamento del dato o deindicizzazione del risultato di ricerca), bensì anche la qualità degli interessi in bilanciamento: nel caso di istanza che vada ad incidere sulla sostanza delle informazioni, non pare possibile identificare un contro-interesse della collettività alla conoscenza del dato obsoleto, ma anzi v'è una sostanziale convergenza tra finalità dell'interessato e quella dell'utente che aspira alla completezza e correttezza dei dati rinvenuti in Rete. Al contrario, come visto, nel caso di mera deindicizzazione del risultato di ricerca, il diritto del singolo utente rischia di frustrare, peraltro in assenza di contraddittorio reale, quello alla informazione della collettività. Dunque, in considerazione di tanto e della delicatezza degli interessi contrapposti, il procedimento di rimozione del risultato di ricerca, ancor più di quello di aggiornamento sostanziale del dato presente sulla pagina sorgente, dovrebbe essere caratterizzato dalla necessaria presenza di un soggetto, magari di matrice pubblicistica (o parapubblicistica), che assicuri il rispetto della libertà d'accesso alle informazioni presenti sul *web*⁵⁰.

8. Conclusioni

Pur nella consapevolezza delle evidenti differenze tra le descritte procedure del DMCA e quelle oggi elaborate, in autonomia, dai gestori dei motori di ricerca, specialmente in relazione all'interesse tutelato (proprietà intellettuale contro diritti alla riservatezza, alla tutela dei dati personali ed all'identità personale), il confronto tra i modelli può offrire comunque interessanti spunti di riflessione. In primo luogo, come già rilevato, la procedura di *notice and take down* statunitense si caratterizza per un elevato grado di coordinamento con il dato normativo. La procedura di rimozione proposta oggi dai motori di ricerca sulla scorta dei principi fissati dalla sentenza della Corte di giustizia, come d'altronde tutte le diverse procedure di stampo autoregolamentare apprestate dai maggiori *players* che offrono servizi su Internet⁵¹, si sostituisce, almeno in parte ed in prima istanza, ai rimedi tradizionali, tra i quali, come in questo caso, il ricorso all'Autorità amministrativa indipendente. Finisce così per realizzarsi, di fatto, una sorta di concorrenza tra i vari strumenti di tutela,

⁵⁰ Cfr. A. LOPEZ-TARRUELLA, *The International Dimension of Google Activities: Private International Law and the Need of Legal Certainty*, in ID. (ed.), *Google and the Law*, cit., pp. 329 ss.

⁵¹ Si pensi, a titolo esemplificativo, al ContentID di YouTube.

non coordinati e armonizzati tra di loro.

La procedura introdotta dal DMCA, inoltre, si svolge secondo tempistiche ben definite e contingentate, con una scansione puntuale delle sue diverse fasi: il generico riferimento ad un «*vaglieremo la sua richiesta il più presto possibile*», connessa alla prospettazione di un possibile affollamento dato da un repentino accumularsi dei reclami dimostra come la procedura di rimozione offerta oggi dai motori di ricerca sia ancora lontana da standard certi di efficacia ed effettività. Il problema più rilevante, in ogni caso, consiste, senza dubbio alcuno, nell'assenza di una qualsivoglia garanzia di un contraddittorio minimo: il prestatore non è obbligato ad agevolare un indiretto 'dialogo' tra l'autore della *notification* ed i soggetti titolari dell'opposto interesse alla permanenza del contenuto (identificabili vuoi nel titolare del sito sorgente, vuoi nella collettività degli utenti, vuoi ancora in un soggetto che pure abbia una posizione qualificata rispetto alla medesima informazione da deindicizzare), ma il più delle volte svolgerà direttamente un sommario bilanciamento valoriale agendo in via immediata sull'informazione, decidendo di oscurarla o di preservarne la visibilità. In sede di procedura infatti non è assicurato—né tanto era stato d'altronde ipotizzato dalla Corte di giustizia—il benché minimo coinvolgimento di possibili contrapposti interessati alla immediatezza d'accesso alla notizia. Si potrebbe osservare, sul punto, come il numero degli interessati possa essere per certi versi indeterminato, ma invero facilmente individuabile: si pensi ad esempio allo stesso editore del sito sorgente, che per precise ragioni non abbia 'scremato' l'informazione attraverso i protocolli di esclusione, o ancora si guardi ad ulteriori individui coinvolti nella medesima vicenda che l'interessato mira ad oscurare.

In definitiva, la circostanza per cui sia soltanto il motore di ricerca ad agire, sperando di fatto una funzione paragiudiziale (non sovrapponibile a quella di garante e, per certi versi, di 'facilitatore' invece imposta dal DMCA), rischia di relegare la fase del bilanciamento ad una mera verifica della sussistenza dei diritti dell'interessato, mediati poi dall'interesse economico del prestatore a non vedere aumentare i costi di gestione delle già numerosissime istanze⁵².

Un altro elemento di allarme attiene all'assenza di un valido strumento di *deterrence* avverso eventuali comportamenti dolosi dei *claimants*: la *copyright misrepresentation* è il perno su cui ruota l'efficienza e il corretto funzionamento dell'intero sistema di notifica e rimozione approntato dal DMCA⁵³. Nulla di

⁵² A pochi giorni dalla sentenza, secondo il Financial Times, il più diffuso motore di ricerca del mondo avrebbe ricevuto oltre 41 mila istanze di rimozione (www.ft-com).

⁵³ Cfr. L.P. LOREN, *Detering Abuse of the Copyright Takedown Regime by Taking Misrepresentation Claims Seriously*, cit. Sui rapporti tra *fair use* e procedure di *notice and take down*, v. I.S. NATHENSON, *Looking for Fair use in the DMCA's safety dance*, in Akron

analogo esiste oggi in materia di rimozione dei *link* indesiderati dai risultati di ricerca. La sistematica rimozione delle informazioni svolta dai prestatori potrebbe così essere preceduta ed affiancata dall'aumento esponenziale di richieste false o non adeguatamente motivate da parte degli interessati, amplificando l'effetto censorio e limitativo della libera apprensione di informazioni sul *web* favorito dall'utilizzo dei motori di ricerca.

Peraltro, anche la procedura di aggiornamento/rettifica di contenuti obsoleti, ipotizzata dalla Suprema Corte italiana e posta direttamente a carico dei titolari dei siti sorgente, è circondata da incertezze assolutamente analoghe in ordine a modalità e tempi di svolgimento al fine di dar risposta alle istanze degli utenti. D'altro canto, deve pur rilevarsi come il diritto alla deindicizzazione di determinati risultati di ricerca associati al proprio nome, per come fondato dalla Corte di giustizia, completamente slegato nel proprio esercizio da qualsivoglia elemento di pregiudizio in capo all'interessato, allo stato, rischi di minare profondamente l'attendibilità dei contenuti del *web*, con circolazione di verità dimidiate offerte agli utenti 'a macchia di leopardo'.

Si potrebbe giungere, dunque, al paradosso, per larghi tratti antistorico e privo di prospettiva, per cui, indipendentemente dagli accadimenti della vita reale, ciascun individuo possa decidere arbitrariamente quali verità debbano emergere e quali no allorché il suo nome venga inserito quale *query* in un motore di ricerca. In altre parole, un'abdicazione della verità storica in favore di un diritto dai confini, ad oggi, troppo labili ed incerti per non far presagire il rischio pressante di abusi e distorsioni: ogni soggetto potrebbe finire per imporre, nel *web*, spazio destinato a divenire sempre più centrale ai fini della formazione delle coscienze e delle conoscenze, una rappresentazione di sé e del proprio passato (più o meno prossimo) lontana dalla realtà.

Possono il diritto e la tecnologia essere legittimamente impiegati per mutare non il passato, ma la rappresentazione dello stesso, tramite processi di arbitraria selezione? La domanda, densa di inquietudini, richiama alla mente un altro passaggio del celebre scrittore ceco ricordato in apertura dello scritto: «*gli uomini vogliono essere padroni del futuro solo per poter cambiare il passato*»⁵⁴.

Int. Prop. J., 3, 1, 2009, pp. 121-170.

⁵⁴ Tratto da «*Kniha smíchu a zapomnění*», edito nel 1978 e pubblicato in Italia, nel 1980, con il titolo «*Il libro del riso e dell'oblio*» (trad. di Serena Vitali).

Abstract

As recently decided by ECJ, the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful. The paper analyzes this obligation of deletion, imposed by ECJ on the operators of search engine, in the perspective of the need to reconcile the right to free access to information and the right to privacy and to the protection of personal data. Specifically, the Authors focus on contents of the instance proposed by the data subject and on the (hybrid) role assigned by ECJ to the operator of a search engine. Further, the authors compare the procedure of deletion established by ECJ with the notice-and-take-down model introduced by DMCA and with a recent judgment of Italian Supreme Court (Cass. n. 5525/2012) on the right to update personal data found online.

Cosimo Comella

Indici, sommari, ricerche e aspetti tecnici della 'de-indicizzazione'

SOMMARIO: 1. Introduzione - 2. *Searching and sorting* - 3. Indici e sommari della rete - 4. I motori di ricerca web - 4.1. Sviluppo dei motori di ricerca - 4.2. Indici e sommari nel modello di Google Search - 5. Memoria della rete e controllo dei dati - 5.1. Aggiornamento delle notizie e coerenza dell'indice - 5.2. Controllo delle informazioni indicizzabili - 5.3. Il Robots Exclusion Protocol - 5.4. Limitazioni del Robots Exclusion Protocol - 5.5. Effetti paradossali. - 5.6. Controllo di accesso con autenticazione o con liste ACL - 5.7. Uso dei Captcha o di fasi interattive - 5.8. Il web semantico e il controllo delle informazioni - 6. Diritto all'oblio e motori di ricerca nell'esperienza del Garante - 6.1. Reputazione online e diritto all'oblio - 6.2. Google e la sentenza Google Spain - 7. Conclusioni

«Lo recuerdo (yo no tengo derecho a pronunciar ese verbo sagrado, sólo un hombre en la tierra tuvo derecho y ese hombre ha muerto) con una oscura pasionaria en la mano, viéndola como nadie la ha visto, aunque la mirara desde el crepúsculo del día hasta el de la noche, toda una vida entera». (Funes el Memorioso, J.L. Borges)

1. Introduzione

Avere a disposizione strumenti efficienti per l'individuazione e il reperimento di informazioni sulla rete è stata sempre una necessità avvertita dalla comunità informatica e dagli sviluppatori di Internet anche prima dello sviluppo e della diffusione della tecnologia e dei servizi World Wide Web. Oggi questi strumenti, che spaziano dai semplici metodi di accesso ai più sofisticati sistemi di *information retrieval*, conoscono il loro apice di successo, anche commerciale, nella tecnologia dei motori di ricerca, cui si affiancano altri sistemi più specialistici di *business intelligence* e di analisi dei dati secondo il paradigma dei *big data*.

La loro applicazione a informazioni di carattere personale, insieme alla ubiquità e pervasività di Internet e alla semplicità d'uso degli strumenti di

ricerca accessibili al pubblico, espongono tuttavia l'individuo alla perdita di controllo sui propri dati personali, che possono entrare a far parte di una sorta di memoria permanente della rete contro la volontà e all'insaputa degli interessati a cui sono riferiti (il cosiddetto *inconscio digitale*). In questi casi tentare di sottrarsi all'invadenza di una continua proiezione e propagazione in rete di informazioni per effetto dei *search engines* può avere perfino effetti paradossali, contribuendo all'ulteriore diffusione di notizie o dati di cui si vorrebbe limitare la conoscibilità. Nel seguito verranno esposti i principali strumenti disponibili, con le attuali tecnologie, per esercitare una qualche forma di controllo, anche *ex post*, sui dati pubblicati con la tecnologia *web* in Internet, discutendone l'efficacia e le limitazioni.

2. *Searching and sorting*

Le tecniche di ricerca e di indicizzazione delle informazioni hanno sempre costituito un primario campo di ricerca per i *computer scientist* fin dagli albori dell'informatica, soprattutto nella forma di metodi di accesso a informazioni strutturate organizzate in grandi *data base* oppure in quella di algoritmi di ricerca in strutture dati, con applicazioni e ricadute tecnologiche su tutta l'informatica, dall'elettronica dei circuiti logici ai sistemi operativi, dal *software* di base fino alle applicazioni, alle reti distribuite e ai servizi di *cloud computing*. Non a caso Donald E. Knuth dedicò al tema degli algoritmi di ricerca, nel 1973, il terzo volume della sua opera fondamentale *The Art of Computer programming*¹, iniziata nel 1962: gli algoritmi di ricerca, al pari di quelli di ordinamento e di altri algoritmi fondamentali, sono alla base non solo della formazione degli studiosi ma anche del funzionamento di quasi tutto il *software* che quotidianamente adoperiamo o che viene utilizzato per far funzionare i servizi della società dell'informazione. Il problema della ricerca efficiente di dati in grandi archivi, siano essi strutturati in *database* ovvero non strutturati e consistenti in raccolte di informazioni di vario tipo e formato o in informazione sparsa, è quindi centrale nell'informatica e non nasce con Internet o con il *web*, anche se con questi si trasforma da problema meramente tecnologico in fenomeno sociale ed economico².

¹ D. E. KNUTH, *The Art of Computer programming*, vol. 3, *Sorting and Searching*, Addison-Wesley, 1973.

² Hal R. VARIAN, *The Economics of Internet Search*, Rivista di Politica Economica, November-December 2006.

3. Indici e sommari della rete

Problema comune a tutte le tecniche di *information retrieval* è il descrivere opportunamente l'informazione da cercare e, sulla base di una metrica predefinita, che consenta di calcolare la distanza dei possibili risultati dal *target* di ricerca, individuare la collocazione delle informazioni corrispondenti o correlate a quella cercata nell'ambito di raccolte dati di elevata dimensione.

Al crescere del volume di informazioni disponibili per la consultazione in rete, equiparabili ormai per vastità a quella *Biblioteca di Babele* immaginata da Jorge Luis Borges³, l'importanza degli indici e dei metodi di catalogazione e recupero selettivo delle informazioni è determinante per la fruizione della rete come serbatoio di conoscenza a disposizione dell'individuo.

Nello sviluppo di Internet già la fruizione efficiente di alcuni servizi di rete poneva dei problemi di indicizzazione e di efficiente recupero di informazioni senza un controllo centrale: in questa fase nasce il *Domain Name System* (DNS)⁴, sistema di *naming* distribuito che consente tuttora, con estrema efficienza, di cercare e recuperare informazioni (indirizzi IP, nomi a dominio, informazioni tecniche) necessarie alla comunicazione in rete tra utenti e tra sistemi.

Più vicini ai *search engines* oggi utilizzati sono i primi strumenti di indicizzazione di file e documenti accessibili nella rete Internet prima dell'avvento del *World Wide Web*, che conobbero la loro massima espansione nei primi anni '90 con i servizi *Archie* e *Veronica*.

Mentre il primo⁵ consentiva di selezionare gli *FTP (File Transfer Protocol) server* che mettevano a disposizione per il *download*, con la 'modalità anonima' di trasferimento dei file (*anonymous ftp*), i documenti digitali o codici programmatici di vario tipo cercati in base al nome del rispettivo file o alla eventuale sua descrizione, con *Veronica*⁶ era possibile effettuare ricerche nel cosiddetto *GopherSpace*, ovvero tra i documenti multimediali accessibili sui *Gopher server* sparsi in Internet e che costituirono un primo esempio funzionante di rete ipertestuale di dimensione

³ J.L. BORGES, *La biblioteca de Babel*, in *Ficciones*, SUR, 1944.

⁴ P. MOCKAPETRIS, Internet Protocol Suite RFC 882, *Domain Names – Concepts and Facilities*, November 1983.

⁵ P. DEUTSCH, *Archie - An Electronic Directory Service for the Internet*, Computing Centre, McGill University, 1990.

⁶ S. FOSTER - F. BARRIE, *Very Easy Rodent Oriented Netwide Index to Computerized Archives*, University of Nevada, Reno, 1992.

globale che precedette il *World Wide Web*. Analogamente, il problema della ricerca si era posto già rispetto all'enorme mole di informazioni contenuta nella rete di notizie *Usenet*, sviluppatasi a partire dal 1979 indipendentemente da Internet/ARPAnet e basata inizialmente su protocolli UUCP (*Unix-to-Unix Copy Program*). Con il *porting* di Usenet sui protocolli TCP/IP di Internet la richiesta di più ampie funzionalità di ricerca nelle *news* produsse diversi sistemi, il più famoso dei quali è stato il servizio *DejaNews* accessibile tramite *web*.

«Remember - your current or future employers may be reading your articles. So might your spouse, neighbors, children, and others who will long-remember your gaffes».

(da «Hints on Writing Style For UseNet», *post* permanente nel gruppo di discussione Usenet *news.announce.newusers*, 1991)

Proprio la formazione di questo primo grande archivio *online* dei c.d. *post* circolati sulla rete Usenet dal 1981 in poi⁷ pose su larga scala i primi problemi di *privacy* (così come di diritto d'autore relativamente alla diffusione di contenuti protetti da *copyright* attraverso le cosiddette gerarchie *alt.binaries*.)^{*} relativi alla ripubblicazione e all'accresciuta diffusione di messaggi i cui autori, nonostante i *caveat* presenti già nei *tutorial* per l'uso della rete, non si rendevano conto dei fattori moltiplicativi legati alla circolazione globale delle notizie. Men che meno essi potevano immaginare l'ulteriore diffusione, via *web*, di messaggi affidati anni prima al sistema dei *newsgroups*, quando Usenet era utilizzata da una relativamente ristretta cerchia di utenti e prevedeva l'utilizzo di *software* specifico per la consultazione e la creazione delle *news*.

4. I motori di ricerca web

4.1. Sviluppo dei motori di ricerca

La diffusione del *World Wide Web*, divenuto fenomeno di massa dal 1994-1995, ben presto amplificò le esigenze di recupero di informazioni, sia per l'ampiezza della rete ipertestuale che si andava sviluppando, sia per la varietà di contenuti e di formati digitali in essa reperibile: testi, docu-

⁷ Tale servizio è stato acquisito da Google nel 2001 ed è entrato a far parte, come *Google Groups*, dei servizi offerti agli utenti del motore di ricerca.

menti, immagini, filmati, registrazioni sonore, file di ogni tipo e natura. Da qui parte il forte sviluppo della tecnologia dei motori di ricerca, basato sui risultati scientifici conseguiti nei decenni precedenti nel campo degli algoritmi dell'*information retrieval* e dei *data base management systems*. I motori di ricerca via via resi accessibili al pubblico di Internet vengono utilizzati tramite l'inserimento di parole chiave testuali, che possono anche essere composte tra loro tramite operatori logici (perché derivati dalla logica booleana), per formare delle complesse *query strings*. Al di là di quale sia l'oggetto della ricerca, sia esso quindi un contenuto documentale testuale o multimediale, lo strumento di ricerca è di tipo *text-based*, perché prevede un'interazione basata sull'inserimento di stringhe di caratteri e sulla loro successiva ricerca all'interno di contenuti pubblicati.

Strumenti più avanzati consentono di cercare un'informazione a partire da chiavi non soltanto testuali: per la ricerca di immagini in rete può infatti essere più adatto uno strumento che permetta di inserire come chiave una fotografia o un altro contenuto digitale (filmati, registrazioni sonore...) per cui si vogliano trovare delle corrispondenze, piuttosto che inserire delle parole da confrontare con etichette di testo (*tags*) che talvolta arricchiscono la descrizione dei contenuti digitali presenti in rete. Ai motori di ricerca testuali si affiancano dei sistemi di ricerca più evoluta, che consentono di specificare l'oggetto della ricerca in linguaggio naturale o prossimo al linguaggio naturale. Nell'esperienza della maggior parte degli utenti il concetto di motore di ricerca è però attualmente associato all'utilizzo di funzionalità di ricerca testuale, per parole-chiave, proposto in rete da servizi *online* quali Excite, Altavista, Yahoo!, Bing e altri, fino a Google, maggiore operatore del settore. Quest'ultimo, abbinando la raccolta pubblicitaria (caratterizzata da originali sistemi di fissazione del prezzo per i contratti di *advertising*)⁸ a una notevole efficienza nel fornire i risultati delle ricerche, ha assunto una tale posizione dominante, soprattutto nel contesto europeo, da poter essere assunto come riferimento per una discussione sulle implicazioni di *data protection* che scaturiscono, in generale, dalla tecnologia dei *search engines* in Internet. Anche a causa di queste caratteristiche di efficienza tecnica e di forza di mercato, il servizio Google Search è stato al centro di diversi casi giudiziari, fino alla recente decisione della Corte di giustizia dell'Unione Europea in tema di diritto all'oblio nel c.d. *caso Google Spain*.

⁸ M.NALDI, G. D'ACQUISTO, G. F. ITALIANO, *The value of location in keyword auctions*, in *Electron. Commer. Rec. Appl.* 9, 2 (March 2010), pp. 160-170.

4.2. Indici e sommari nel modello di Google Search

Il funzionamento di Google Search, come quello di analoghi servizi, è basato sull'utilizzo di un agente automatico, detto *spider* o *crawler*, per la raccolta delle pagine *web* accessibili *online*, esplorate tramite algoritmi di visita su grafi che consentono di percorrere tutte le diramazioni della rete di riferimenti ipertestuali in modo efficiente. Il buon esito di una ricerca presuppone quindi che il contenuto cercato sia stato oggetto di 'visita' da parte dello *spider* affinché i dati contenuti nelle pagine ispezionate possano popolare la gigantesca *cache*⁹ del motore di ricerca ed essere lì indicizzati e resi disponibili per la consultazione. Essenziale per l'efficacia del servizio di ricerca è la determinazione della *frequenza di visita* dei diversi siti: stime della stessa Google fanno ritenere che, in assenza di *input* specifici, occorranzo diverse settimane o anche mesi per ottenere un completo *refresh* della *cache*, ottenibile con una visita esaustiva della *websphere* tramite gli *spider*. Va da sé che i siti più visitati dagli utenti, più ricchi di contenuti in continuo aggiornamento e più citati tramite *link* ipertestuali (HREF o *hypertext reference*) sono quelli più frequentemente ispezionati dalle sonde di indicizzazione.

5. Memoria della rete e controllo dei dati

5.1. Aggiornamento delle notizie e coerenza dell'indice

Oltre a rendere disponibili le informazioni su cui costruire l'indice e far funzionare l'algoritmo di ricerca, la presenza di una memoria *cache* a supporto di un *search engine* permette di presentare all'utente un'anticipazione del risultato completo in forma di riassunto (*summary*). Laddove si verifichi un disallineamento tra il contenuto presente in *cache* e la pagina originaria, la *cache* fornirà una visione non aggiornata del contenuto pubblicato, che potrebbe esser stato modificato o anche rimosso dal sito di originaria pubblicazione. Per questo motivo, è fondamentale minimizzare i tempi di esposizione a consultazione di risultati non aggiornati, associando una sorta di 'misura di freschezza' alle informazioni caricate nell'indice. Le modalità con cui questa misura viene calcolata costituiscono oggetto

⁹ Memoria veloce in grado di assicurare l'immediata disponibilità di un dato presente a livello inferiore in una struttura a gerarchia di memoria.

di ricerca nel campo della *computer science*, con diverse differenti proposte rinvenibili in letteratura^{10 11}.

Quando una notizia indicizzata da un motore di ricerca riporta informazioni riferibili a un individuo, la misura tecnica della freschezza dell'indice è anche, in qualche modo, misura del corretto trattamento dei dati personali dell'interessato: l'aggiornamento delle informazioni riferibili agli individui è uno dei valori della protezione dei dati personali, anche nell'ordinamento italiano, laddove l'articolo 11 del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196) prevede che i dati personali oggetto di trattamento siano «esatti e, se necessario, aggiornati».

Benché la responsabilità di mantenere informazioni esatte e aggiornate gravi *in primis* su chi le ha pubblicate per primo, l'attività di indicizzazione e di *caching*, con la successiva presentazione di risultati in forma di sommario, è molto vicina, o del tutto coincidente, a una vera e propria ripubblicazione delle stesse informazioni, con tutte le implicazioni che da ciò possono derivare in tema di responsabilità del *publisher* e di doveri rispetto all'esercizio dei diritti degli interessati.

Il motore di ricerca Google ha messo a disposizione degli utenti delle apposite sezioni (*Google Webmaster Tools*) per segnalare la presenza nell'indice di *link* a pagine non più esistenti oppure modificate e perciò non coerenti con le chiavi di ricerca o che presentano nel *summary* delle notizie non aggiornate, differenti da quelle correntemente *online* sul sito di originaria pubblicazione. In assenza di segnalazione il motore di ricerca potrebbe impiegare anche alcuni mesi prima di accorgersi che una data pagina sia stata modificata o addirittura rimossa, con ritardo dipendente da molti fattori, tra cui la popolarità della notizia e del sito che la pubblica.

La richiesta di rimozione di pagine non più esistenti o il loro aggiornamento non richiede di essere utenti registrati ed è accessibile in italiano all'indirizzo <https://www.google.com/webmasters/tools/removals?pli=1>.

Analoghi strumenti sono messi a disposizione da altri motori di ricerca, come *Yahoo Search* e *Bing* che offrono ai propri utenti i *Bing Webmaster Tools* e i *Content Removal Tools*¹² tramite cui è possibile rimuovere elementi della *cache* scaduti o i c.d. *broken links*.

¹⁰ J. CHO - H. GARCIA-MOLINA, *Synchronizing a database to improve freshness*, in Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, Dallas, Texas, 2000, pp. 117-128.

¹¹ E. G. COFFMAN JR - Z. LIU - R.R. WEBER, *Optimal Robot Scheduling for WebSearch Engines*, 1 *Journal of Scheduling* pp. 15-29 (1998).

¹² <http://www.bing.com/webmaster/help/bing-content-removal-tool-cb6c294d> [consultato il 30/09/2014].

5.2. Controllo delle informazioni indicizzabili.

Già a partire dalla seconda metà degli anni '90 la comunità Internet rese disponibili strumenti che permettevano di affrontare l'esigenza, sentita per lo più dai gestori di siti *web*, di limitare la possibilità da parte dei motori di ricerca di indicizzare i contenuti pubblicati *online* e non protetti con accorgimenti di sicurezza, perché lasciati intenzionalmente disponibili per la consultazione da parte di chiunque. L'esigenza di escludere alcuni contenuti dall'azione invasiva dei motori di ricerca aveva originariamente motivazioni del tutto differenti da quelle che oggi appaiono più rilevanti: in un'era, quella degli anni '90, caratterizzata da un livello di prestazioni dei sistemi informatici di almeno due ordini di grandezza inferiore rispetto a quello dei sistemi odierni (a parità di categoria)¹³, era necessario evitare il sovraccarico dei *server* derivante dalle connessioni intensive degli *spider* dei motori di ricerca, soprattutto quando queste non avrebbero poi potuto produrre risultati apprezzabili in termini di arricchimento degli indici, per la presenza di contenuti difficilmente indicizzabili, ovvero poveri di testo (immagini, video, audio...).

Escludere dalla visita degli *spider* alcune porzioni dei *filesystem* che ospitavano le pagine e i *file* accessibili tramite il protocollo *http* (*Hypertext Transfer Protocol*)¹⁴ diventava allora una questione di *performance* significativa, soprattutto per siti con grandi basi documentali.

La capacità di controllare l'indicizzazione e quindi la diffusione ulteriore di dati pubblicati in rete, generata o amplificata dall'azione dei motori di ricerca, è oggi invece più importante per assicurare quel *right to be forgotten*, che costituisce uno dei punti più importanti della proposta di regolamento europeo sulla protezione dei dati personali presentata dalla Commissione Europea nel gennaio 2012¹⁵. A questo proposito, la *European Union Agency for Network and Information Security* (ENISA) ha

¹³ Una differenza di un fattore 100 è riscontrabile sia nei livelli di integrazione, espressi in numero di transistor per circuito, sia nella frequenza di clock delle CPU su microprocessore, passata dagli 8 MHz del 1988 al GHz del 2001.

¹⁴ Inizialmente pubblicato come HTTP V0.9, il protocollo venne standardizzato da IETF con la pubblicazione dello IPS RFC 1945 «Hypertext Transfer Protocol -HTTP/1.0» nel maggio 1996.

¹⁵ Proposta di Regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati). 25/01/2012. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:IT:PDF>. [consultato il 30/09/2014].

pubblicato già nel 2011 un primo interessante rapporto sugli strumenti tecnici disponibili per implementare quel diritto nel contesto della pubblicazione in rete o dell'uso di dati personali nei sistemi informativi¹⁶.

Tradurre con strumenti tecnici efficaci e accessibili alla maggior parte degli utenti delle rete, e anche agli interessati che non la utilizzano, l'esercizio dei propri diritti in tema di dati personali costituisce comunque una sfida tecnica di grande portata, che solo da qualche anno vede i principali gestori di *search engines* impegnati nello sviluppo di apposite funzionalità da integrare nei propri servizi *online*.

5.3. *Il Robots Exclusion Protocol*

Lo strumento sviluppato dalla comunità Internet negli anni '90 è stato il *Robots Exclusion Protocol* (REP)¹⁷, ovvero una sorta di convenzione tecnica di cui, da una parte, gli sviluppatori di *software* per servizi *web* e, dall'altra parte, i programmatori delle funzioni di indicizzazione dei principali motori di ricerca possono tener conto nella realizzazione dei rispettivi prodotti, affinché la visibilità dei contenuti di un sito tra i risultati di una ricerca sia modulabile dal gestore tramite la compilazione di un *file* di tipo testuale denominato *robots.txt* e presente nella *root directory* dei *web server* in modo tale da poter essere letto all'indirizzo <http://nome.a.domini.del.sito/robots.txt>.

Il formato di robots.txt

Il file *robots.txt* contiene dei *record* raggruppati in sezioni introdotte dal campo *User-agent* seguito da uno o più direttive *Disallow*.

Il campo *User-agent* indica a quale *search engine* le direttive successive sono rivolte. La sua sintassi è:

User-agent:<spazio><nome dello spider>

La direttiva *Disallow* serve a indicare allo *spider* indicato nel campo *User-agent* quali *pagine* o *directory* non può acquisire, con la sintassi seguente:

¹⁶ Il rapporto è disponibile sul sito di Enisa all'indirizzo: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport [consultato il 30/09/2014].

¹⁷ M. KOSTER, *A Standard for Robot Exclusion*, 30/06/1994 (testo originale in <http://www.redhat.com/support/resources/faqs/RH-apache-FAQ/misc/norobots.html>) [consultato il 30/09/2014].

Disallow:<spazio><nome file o nome directory>

I nomi dei *file* o delle *directory* sono espressi come indirizzi relativi, nel *filesystem* del *server* che ospita le pagine *web*, alla *home directory* dei contenuti del sito, indicata da un carattere *slash* (/).

Il campo User-agent può contenere un asterisco (*) per significare ‘qualunque spider’.

User-agent: *

Disallow: /pagina/da_non_indicizzare.html

Disallow: /pagine/da_non_indicizzare/

Il campo *Disallow* può contenere anche un singolo carattere *slash* a indicare ‘qualunque *file* o *directory*’, oppure può essere lasciato vuoto, per indicare che non ci sono pagine sottratte all’indicizzazione.

Il REP prevede che ogni richiesta di acquisizione di una pagina *web* da parte di uno *spider* debba essere preceduta dalla verifica di non inclusione dell’indirizzo della pagina stessa nella ‘lista di esclusione’ del sito, descritta proprio dal contenuto del *file robots.txt*.

Il REP prevede anche altre modalità di esclusione, tra le quali il ricorso ad appositi *metatags noindex* da incorporare nelle pagine Html al fine di interrompere il percorso di visita degli agenti di indicizzazione, impedendo che questi seguano i *link* ipertestuali presenti nelle pagine in forma di *tag* HREF (*Hypertext Reference*).

In molti casi l’efficacia di funzionamento del REP è rafforzata dall’utilizzo congiunto di tutte e due le tecniche.

Azioni preventive alla pubblicazione

Qualora si sia in presenza di dati non ancora pubblicati, e perciò non presenti in nessun indice di ricerca, il *file robots.txt* può essere predisposto in modo opportuno affinché la notizia o la pagina web che si sta per inserire non venga acquisita dagli agenti di ricerca. L’indicazione delle pagine da non indicizzare non deve essere necessariamente puntuale, ma può comprendere tutti i documenti presenti in una cartella, o *directory*, di *filesystem*.

È evidente che l’utilizzo di indirizzi puntuali può più facilmente generare gli effetti paradossali cui si è fatto cenno prima, prestandosi anche a un’analisi perfino solo visiva del *file robots.txt*.

Lo stesso accade inserendo nel *file* l’indicazione delle *directory* da escludere laddove queste abbiano nomi immediatamente riferibili al loro contenuto.

Una volta compreso l'indirizzo della pagina tra quelli da non indicizzare, si può procedere alla pubblicazione *online* del contenuto, con ragionevole aspettativa — se la configurazione del *robots.txt* è stata correttamente realizzata — che né Google Search, né Yahoo né gli altri principali servizi di indicizzazione e ricerca web saranno in grado di acquisirlo e indicizzarlo.

Azioni a posteriori

Nel caso in cui un certo contenuto sia stato già indicizzato perché pubblicato e non escluso, in un primo momento, dall'indicizzazione tramite gli strumenti del REP, e lo si voglia rimuovere dai risultati di un motore di ricerca occorrerà agire su più fronti.

In primo luogo occorrerà configurare opportunamente il *robots.txt* o utilizzare i *metatag noindex* per segnalare che una pagina o dei *link* ipertestuali non devono essere visitati e indicizzati.

Successivamente occorrerà agire presso i motori di ricerca affinché i riferimenti alla pagina in questione siano espunti dai rispettivi indici. Nel caso di Google, la società ha predisposto, nell'ambito dei Webmaster Tools, oltre alla possibilità di richiedere la rimozione dall'indice di riferimenti a pagine non più esistenti o per le quali sia stata modificata la visibilità da parte degli *spider* di ricerca, anche l'aggiornamento dei riferimenti a seguito di modifiche apportate ai documenti indicizzati.

5.4. Limitazioni del Robots Exclusion Protocol

Come accennato, nonostante il nome, il REP non è un vero protocollo, né *standard* cui l'industria del *software* debba necessariamente attenersi. Non vi è quindi garanzia, pur in presenza di una corretta configurazione del *robots.txt*, che una certa pagina non venga indicizzata da un qualsiasi motore di ricerca, se la si vuole mantenere comunque accessibile via *web* a un pubblico indeterminato.

D'altra parte, anche i più avanzati motori di ricerca non rispettano pienamente il REP, limitando in molti casi l'efficacia dello strumento e sminuendone l'importanza. Per quanto riguarda Google, le azioni per limitare l'indicizzazione dei contenuti di siti *online* si sono basate sulla conformità del motore di ricerca al REP, anche se il livello di *compliance* è

stato soltanto parziale. Probabilmente un'applicazione più rigorosa e più efficace del REP avrebbe permesso una più agevole modulazione della visibilità di alcune informazioni nei risultati di ricerca e avrebbe consentito all'azienda di non subire gli effetti di una decisione molto severa e di difficile attuazione come quella recente della Corte di giustizia UE con cui l'azienda americana, insieme ad altre parimenti interessate, si sta confrontando in queste settimane.

La stessa Google chiarisce, nella *Google's webmaster documentation*, quale sia l'attenzione rivolta a questo sistema di gestione delle indicizzazioni, fornendo le seguenti indicazioni:

«Blocking Google from crawling a page is likely to decrease that page's ranking or cause it to drop out altogether over time. It may also reduce the amount of detail provided to users in the text below the search result. ... However, robots.txt Disallow does not guarantee that a page will not appear in results: Google may still decide, based on external information such as incoming links, that it is relevant.»

Sempre nelle pagine informative del centro di supporto per i *webmaster* di Google si può leggere il seguente avviso:

«While Google won't crawl or index the content of pages blocked by robots.txt, we may still index the URLs if we find them on other pages on the web. As a result, the URL of the page and, potentially, other publicly available information such as anchor text in links to the site, or the title from the Open Directory Project (www.dmoz.org), can appear in Google search results.» (dal Webmaster Tools Help Center di Google)

La parziale efficacia, dovuta all'interpretazione stessa del REP fatta da Google, ha portato evidentemente a risultati insoddisfacenti e che talvolta rivelano proprio l'incorretta implementazione del REP. Basti osservare come a fronte di determinate ricerche con parole chiave alcuni risultati vengano presentati con l'indirizzo URL deprivato del sommario (copia *cache*) con la motivazione seguente:

«A description for this result is not available because of this site's robots.txt — learn more.»

È evidente da questo avviso come, a fronte di un contenuto *online* che, nelle intenzioni del *publisher*, avrebbe dovuto essere sottratto all'indicizzazione da parte dei *crawler* o *spider* dei motori di ricerca (e di ciò è rivelatore l'esplicito riferimento di Google a questa circostanza, anche se in riferimento alla mera assenza del sommario o copia *cache*), questo possa essere nonostante ciò incluso tra i risultati e correlato a determinate parole chiave, rivelando la sua presenza nell'indice di ricerca!

Questo comportamento svela la violazione o la non corretta implementazione del *Robots Exclusion Protocol* da parte di Google. Altro esempio di mancata *compliance* è quello relativo alla riapparizione periodica dei risultati di ricerca che si vorrebbero esclusi: parrebbe infatti che l'efficacia della de-indicizzazione tramite *robots.txt* sia garantita per soli novanta giorni, trascorsi i quali il motore di ricerca riprende a inserire riferimenti alle pagine che l'originario *publisher* vorrebbe in effetti sottratte all'acquisizione dallo *spider*. Non vi è stata finora una chiara posizione di Google rispetto a questa anomalia, che evidenzia una incorretta applicazione del REP, laddove gli indirizzi delle pagine da acquisire dovrebbero previamente essere controllati per verificarne l'eventuale inclusione nel *robots.txt* del sito da visitare. Le pagine escluse tramite *robots.txt* non dovrebbero quindi essere in alcun modo acquisite, mentre Google evidentemente procede alla loro acquisizione salvo provvedere successivamente a gestirne, con propri criteri che non rispecchiano la volontà del *publisher*, la visibilità tra i risultati di ricerca.

Alcuni cenni a questo comportamento si ritrovano nella *knowledge base* del motore di ricerca e suscitano dibattito tra utenti, sviluppatori e l'azienda stessa. Sul piano della *data protection* e delle relazioni con le autorità nazionali europee (DPA) tuttavia Google non ha finora chiarito questo aspetto e non ha fornito spiegazioni soddisfacenti all'evidente anomalia che inficia l'efficacia e quindi la fiducia del pubblico in un meccanismo (il *robots.txt*) già in sé abbastanza debole.

La pubblicazione della sentenza *Google Spain* nel maggio 2014 ha poi fatto momentaneamente diminuire l'interesse per la questione, che però occorrerà chiarire perché lo strumento *robots.txt* continua a essere utilizzato dai siti *web* e consente in qualche misura, se ben realizzato, di modulare la visibilità delle pagine tra i risultati di ricerca a volontà dei *publisher*. Tale possibilità andrebbe mantenuta e meglio realizzata, anche se gli interessati, quantomeno in Europa, hanno adesso nei confronti di Google e degli altri *search engines* sottoposti all'ordinamento comunitario la possibilità concreta di esercitare il proprio diritto alla cancellazione dei dati dall'indice

tramite procedure alternative, del tutto separate da quelle connesse all'uso del *Robots Exclusion Protocol*, e svincolate dallo stato di pubblicazione di una determinata pagina *online*.

5.5. Effetti paradossali

I siti dei maggiori periodici *online* ricorrono da tempo al *robots.txt* inserendovi gli indirizzi delle pagine o delle *directory* che, pur essendo accessibili *online*, non sono da indicizzare. A seconda del tipo di *Content Management System* (CMS) adottato per la gestione dei contenuti e del processo editoriale *online*, l'indicazione della pagine può essere espressiva del loro contenuto. Poiché il file *robots.txt* deve essere leggibile da chiunque, il visitatore curioso può liberamente esaminarne il contenuto e trarne degli spunti per andare a recuperare in seguito notizie che la volontà dell'editore vorrebbe in qualche modo limitate nella conoscibilità.

Da questo punto di vista, l'utilizzo di indirizzi 'brevi' o 'non parlanti', da cui non è possibile desumere il contenuto anche solo indicativo della pagina cui fanno riferimento, evita di generare effetti paradossali di accresciuta attenzione verso ciò che si vuole in qualche modo proteggere. Altri fenomeni di indicizzazione non voluta possono derivare dalla citazione della stessa notizia o del corrispondente *link* ipertestuale in un'altra pagina, esterna al sito di originaria pubblicazione: se il *link* è 'parlante' l'effetto di inclusione nei risultati di ricerca sarà enfatizzato.

L'efficacia del REP sarà poi vanificata dalla ripubblicazione automatica della notizia su altri siti, tramite funzioni di *mirroring* e altre forme di importazione automatica di contenuti *online*. Infine, il ricorso al *robots.txt* può generare specifica attenzione da parte di utenti della rete proprio verso quei contenuti che si era cercato di sottrarre all'indicizzazione, per il solo fatto che essi siano citati in quel *file*.

Esistono, infatti, in rete siti e servizi dedicati a effettuare le ricerche proprio nella parte 'nascosta' del *web*: in questo senso si collocano iniziative che comportano la costruzione di indici specificamente volti a rendere accessibili proprio quelle informazioni a cui i *webmaster* avevano riservato, nelle intenzioni, un minor grado di conoscibilità.

Tra i diversi siti che offrono servizi *online* di questo tipo ha guadagnato recentemente una certa notorietà '*Hidden from Google*'¹⁸, che però è specificamente volto a elencare e permettere di consultare i siti i cui contenuti pubblicati hanno comportato l'attivazione di Google con gli strumenti

¹⁸ <http://hiddenfromgoogle.com/>.

approntati dalla società americana per adempiere alle prescrizioni della Corte di Giustizia UE nel noto caso «Google Spain». Presentato come n'iniziativa contro le azioni censorie sul *web*, permette a chiunque di segnalare notizie che, per effetto della sentenza europea, sono state sottratte alla visibilità tra i risultati di ricerca.

5.6. *Controllo di accesso con autenticazione o con liste ACL*

Le tecniche per la limitazione dell'azione dei motori di ricerca sono molteplici, ciascuna dotata di maggiore o minore efficacia e impatto sulla fruibilità delle informazioni. In primo luogo, chi non voglia conferire alle proprie pubblicazioni *web* una indesiderata pubblicità dovrebbe riflettere seriamente sull'opportunità di mettere *online* quel determinato contenuto in modalità accessibile a chiunque. Il protocollo Http permette infatti la definizione di controlli di accesso tramite la configurazione di un file *htaccess* con cui si può attivare fase di autenticazione con *username* e *password* e si possono definire delle *access control lists* (ACL) con cui abilitare o negare l'accesso a *file* e *directory* del sito in base agli indirizzi di rete di provenienza delle connessioni.

La fase di autenticazione impedisce agli *spider* dei motori di ricerca di proseguire nella visita del sito, mentre la configurazione di ACL selettive impedisce del tutto la connessione di *client* non graditi. Tuttavia effetti avversi si manifestano sull'usabilità del sito e sulla fruibilità da parte del pubblico privo di credenziali di accesso.

Come espediente senza scopi di vera protezione delle informazioni, ma idoneo a sbarrare il percorso di visita di un sito agli agenti di ricerca, viene talvolta utilizzato un *form* per l'autenticazione le cui credenziali sono intenzionalmente pubblicate e conoscibili da chiunque, permettendo l'accesso ai contenuti a un utente ma non a un normale *spider* di un motore di ricerca.

5.7. *Uso dei Captcha o di fasi interattive*

Effetti interdittivi dell'indicizzazione automatica si ottengono proteggendo le pagine *online* con il ricorso a strumenti Captcha (*Completely Automated Public Turing Test to Tell Computers and Humans Apart*) volti specificamente a discriminare tra utenti umani e programmi automatici di raccolta dei dati interagenti con un'applicazione informatica, secondo il

modello del *test di Turing*¹⁹. Pur tenendo conto dell'evoluzione degli strumenti informatici che consentono a volte di superare in modo automatico dei controlli *captcha*, questi possono rappresentare una efficace barriera contro l'utilizzo di programmi automatici e, in particolare, degli *spider* di indicizzazione. Analogamente, anche l'interposizione di una qualsiasi fase interattiva, che può essere rappresentata dalla compilazione di una *form* per la ricerca locale delle informazioni o dal *click* su un tasto *submit* per proseguire la navigazione tra i contenuti di un sito, può permettere di proteggere i contenuti *online* dall'invasività di agenti automatici non graditi.

5.8. *Il web semantico e il controllo delle informazioni*

Con il termine *web semantico*, coniato da Tim Berners-Lee, ideatore del World Wide Web²⁰, ci si riferisce alle tecnologie e ai metodi per arricchire il web trasformandolo in un ambiente in cui i documenti pubblicati vengono collegati a informazioni e dati (*metadati*) che ne descrivono il 'contesto semantico' con formati idonei all'interrogazione e l'interpretazione automatica. Lo sviluppo del web semantico, pur non progredendo secondo le aspettative dei suoi ideatori iniziali²¹, è oggi guidato dal *World Wide Web Consortium* (W3C) e si basa sulla promozione di formati di dato comuni sul *web* in modo da trasformarlo in chiave *datocentrica*, grazie a linguaggi e *framework* descrittivi quali il *Resource Description Framework* (RDF), il *Web Ontology Language* (OWL) e l'*Extensible Markup Language* (XML). Le *ontologie* e i *linked data* costituiscono la base concettuale per la creazione di un nuovo tipo di *web* che renda possibile, tra l'altro, effettuare ricerche molto più sofisticate rispetto ai *search engines* convenzionali, agenti sul livello lessicale del linguaggio, e di creare collegamenti automatici tra documenti e dati andando molto oltre il semplice riferimento ipertestuale, sfruttando la possibilità di penetrare la struttura più profonda, sintattica e semantica, dei dati e dei documenti.

La disponibilità di un livello semantico permette di trattare le differenti porzioni di informazione di cui si compone un documento con flessibilità, disciplinandone il regime di visibilità e protezione dei dati personali, trasformando radicalmente il modo di agire dei motori di ricerca che attualmente indicizzano, in modo che può essere considerato rudimentale,

¹⁹ A.M. TURING, *Computing machinery and intelligence*, in 59 *Mind* pp. 433-460 (1950).

²⁰ T. BERNERS-LEE, *L'architettura del nuovo Web*, Feltrinelli, Milano, 2002.

²¹ N. SHADBOLT, W. HALL, T. BERNERS-LEE, *The Semantic Web Revisited*, IEEE Intelligent Systems, May/June 2006.

tutto ciò che sono in grado di raggiungere *online*.

I *search engines* d'altra parte ricaverebbero enormi vantaggi in termini di efficienza e di accuratezza dei risultati, avvicinando i risultati di ricerca alle aspettative degli utenti ma permettendo, tra le altre cose, di incorporare nei documenti *online* le regole di trattamento nel senso della *data protection*, compresa la validità temporale di un'informazione, la sua riproducibilità o visibilità in indici e sommari.

6. Diritto all'oblio e motori di ricerca nell'esperienza del Garante

6.1. Reputazione online e diritto all'oblio

Il tema del diritto all'oblio è sempre stato all'attenzione del Garante per la protezione dei dati personali fin dalla sua istituzione. All'esito della trattazione di un ricorso relativo alla persistenza in rete, amplificata dai motori di ricerca, di notizie pregiudizievoli per l'attività di un soggetto imprenditoriale che era stato destinatario di una sanzione per pubblicità ingannevole, il Garante nel 2004 prescrisse al titolare del trattamento l'adozione di accorgimenti tecnici per mitigare gli effetti della pubblicazione *online* di notizie sulle sanzioni comminate²² quando la finalità originaria della pubblicazione *online*, ammonitoria e informativa, era venuta meno.

Scopo del provvedimento del Garante era evitare che si realizzasse una sorta di gogna permanente, laddove la pubblicazione per estratto di certe decisioni o sentenze viene tuttora prevista, nel nostro ordinamento, quale pena accessoria, in presenza di un lungo periodo di tempo trascorso dalla sanzione e dal ravvedimento dell'operatore economico.

In base al principio del diritto all'oblio sono stati poi trattati dall'Autorità italiana numerosi casi relativi alla ripubblicazione di notizie negli «archivi storici *online*» dei maggiori quotidiani nazionali. Nei provvedimenti in tema di diritto all'oblio qui citati, e in altri nel tempo adottati, il Garante ha prescritto quale strumento tecnico per adempiere il ricorso al *Robots Exclusion Protocol*, misura idonea, nella maggior parte dei casi, a sottrarre all'indicizzazione da parte dei motori di ricerca le informazioni riferibili a interessati la cui diffusione doveva essere limitata. Sono stati trattati così dei casi di pubblicazione di archivi storici di quotidiani e rivi-

²² <http://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/1116068> [consultato il 30/09/2014].

ste, di diffusione di informazioni personali da parte di soggetti pubblici sulla base di interpretazioni estensive delle norme in tema di trasparenza in ambito pubblico, di pubblicazione di notizie inaccurate o non aggiornate, e perciò lesive della dignità di persone, su quotidiani o riviste *online*.

L'incertezza di giurisdizione e la possibilità di sovrapposizione e conflitto tra differenti giurisdizioni hanno fatto considerare per anni poco praticabile l'imposizione in capo ai gestori dei motori di ricerca di obblighi di espungere dai rispettivi indici i riferimenti a notizie che permangono *online*, pur ledendo diritti degli interessati cui si riferiscono, su sistemi di pubblicazione sottratti alla capacità di intervento delle DPA europee. D'altra parte l'orientamento delle autorità europee di protezione dei dati personali, riunite nel *Working Party* istituito dall'Art. 29 della direttiva 46/95/EU (WP29), rispetto alla titolarità del trattamento dei dati personali è stato costantemente in favore dell'assenza di responsabilità del motore di ricerca, essendo la titolarità del trattamento incardinata sul soggetto che pubblica il contenuto *online* nella sua forma originaria²³. Tale posizione è andata incontro a un importante cambiamento a seguito della sentenza *Google Spain*, cui si fa più compiutamente cenno più avanti, che ha innovato radicalmente la posizione europea in tema di ruoli dei *search engines* nel sistema di protezione dati europeo, di stabilimento del *data controller*, di legge applicabile.

6.2. Google e la sentenza Google Spain

Il motore di ricerca americano si è impegnato nelle scorse settimane per adeguare i propri servizi alla sentenza della Corte di giustizia dell'Unione Europea pronunciata il 13 maggio 2014 riguardo alla causa «Google Spain SL, Google Inc. / Agencia de Protección de Datos (AEPD), Mario Costeja González» (Causa C-131/12)²⁴. La corte europea ha infatti individuato nell'attività di elaborazione delle informazioni svolta dal motore di ricerca un trattamento autonomo, rispetto al quale la società riveste il ruolo di titolare (*data controller*). La sentenza europea costringe oggi Google (e conseguentemente altri operatori che si ritrovino nelle stesse condizioni individuate nella decisione dei giudici europei) ad adottare procedure per cancellare dai propri indici informazioni che possono continuare a essere presenti sul sito di originaria pubblicazione o su altri siti che provvedo-

²³ Si veda in tal senso la «Opinion 1/2008 on data protection issues related to search engines - WP 148» del 4 aprile 2008.

²⁴ In Appendice a questo Volume

no autonomamente alla loro ripubblicazione o citazione. A tal fine, per consentire agli utenti di richiedere la rimozione di talune notizie che li riguardino dai propri indici, Google ha messo a disposizione un modulo *online* nella pagina intitolata «*Search removal request under data protection law in Europe*» raggiungibile all'indirizzo seguente: https://support.google.com/legal/contact/lr_eudpa?product=websearch

Affinché una richiesta da parte di un utente venga presa in considerazione la società richiede che siano verificate tre condizioni: *a*) siano indicati gli indirizzi URL dei link da rimuovere; *b*) sia giustificata la pertinenza delle pagine a cui viene fatto riferimento nell'indice alla persona che presenta la richiesta; *c*) sia spiegato perché quei collegamenti nei risultati di ricerca siano irrilevanti, non aggiornati o in qualsiasi modo inappropriati. Dal punto di vista tecnico si evidenzia la particolare difficoltà di riconoscere in un richiedente la cancellazione un legittimo interessato cui facciano riferimento dati personali pubblicati *online* e indicizzati dal motore di ricerca. A questo proposito Google chiede che il richiedente trasmetta copia di un documento idoneo al riconoscimento di sé o dell'interessato per conto del quale viene presentata la richiesta.

L'adeguamento alla sentenza *Google Spain* pone problemi che vanno ben oltre il mero fatto tecnico, al punto che la società ha annunciato di essersi dotata di un *team* di esperti tecnici e legali di comprovata competenza, che dovrebbe esaminare le richieste di cancellazione da parte di cittadini europei. La decisione della Corte per un verso, relativo alle responsabilità del motore di ricerca, va molto oltre quanto disposto in passato dal Garante italiano con propri provvedimenti che indubbiamente tenevano conto dell'incertezza sulla giurisdizione, oggi risolta con la sentenza europea. Ma le decisioni del Garante riflettevano anche un bilanciamento di interessi tra il diritto all'informazione e alla manifestazione del pensiero, da una parte, e il diritto alla protezione dei dati personali, dall'altra, avendo effetti anche sui siti di originaria pubblicazione. Gli effetti della cancellazione ai sensi della sentenza *Google Spain* appaiono comunque, al momento, parziali: questa è limitata alle versioni del *search engine* rivolte a utenti europei, accessibili attraverso l'uso dei domini Google nazionali (google.it, google.fr...). Alcune informazioni potrebbero quindi essere rimosse o, meglio, non presentate tra i risultati di ricerca a un utente europeo, ma continuare a essere visualizzabili nella versione internazionale del servizio, accessibile nel dominio *google.com*.

La modalità di adempimento di Google appare quindi giocata sulla presentazione dei risultati, e non su radicali interventi sui *database* su cui

è costruito l'indice del motore di ricerca.

Il ristretto intervallo di tempo trascorso dalla decisione della Corte di giustizia UE non consente al momento di valutare pienamente la soluzione che Google (ed eventualmente altri *search engines*) ha messo in atto, poiché è presumibile che questa debba essere ancora affinata e migliorata, sia relativamente all'efficacia della rimozione sia nei criteri di riconoscimento degli interessati e della loro connessione a determinate notizie o dati personali pubblicati ma possibilmente riferibili a una pluralità di differenti soggetti.

Analogamente si presta a controversie la decisione di Google di notificare agli amministratori o *webmaster* le richieste di rimozione di *link* e notizie che si riferiscano a contenuti pubblicati su siti da questi controllati. La scelta è dichiaratamente volta a garantire un equilibrato esercizio dei diritti degli interessati, ai sensi della sentenza *Google Spain*, migliorando il processo decisionale interno alla Società e la resa per gli utenti, ma viene criticata per la possibile violazione della *privacy* di chi si rivolge a Google per la rimozione di notizie dall'indice di ricerca.

7. Conclusioni

Le tecniche di de-indicizzazione *ex post* o di prevenzione dell'indicizzazione sono al momento rudimentali, e tali permangono dalla metà degli anni '90. Strumenti più efficaci del *Robots Exclusion Protocol* sono quelli che prevedono l'utilizzo di fasi di interazione umana con i contenuti *online* prima della loro fruizione da parte degli utenti, in modo da disincentivare, se non escludere del tutto, l'azione di agenti automatizzati di ricerca.

Tuttavia tali accorgimenti non hanno una diffusa accettazione in quanto incidono negativamente sulla *esperienza d'uso* della rete, oggi caratterizzata da una diffusione di dispositivi mobili di ridotte dimensioni e dalla conseguente necessità di garantire una maggiore semplicità d'uso attraverso una semplificazione delle interfacce uomo-macchina.

Altro possibile approccio è quello basato sul paradigma del *web semantico* per la tipizzazione delle informazioni e la definizione di una disciplina del loro utilizzo, anche con riferimento agli aspetti di protezione dati. Tale approccio richiederebbe però un radicale mutamento delle tecniche di pubblicazione *online*, dei formati dei documenti e una conseguente *compliance* da parte dei *search engines*.

Tutto ciò lascia pensare che, qualora si intenda limitare la conoscenza di informazioni l'unico strumento davvero efficace sia la radicale misura della rinuncia alla loro pubblicazione. La presenza sul *web* di una notizia la candida comunque, nonostante le possibili azioni tecniche mitigatrici, a conoscere in misura più o meno rilevante l'indesiderata diffusione, nonostante interventi di legislatori e decisioni giudiziarie che hanno comunque efficacia limitatamente alla giurisdizione esercitabile, in un contesto di fenomeni tecnologici di tipo transnazionale.

Ci si interroga quindi se occorra rassegnarsi a un mondo tecnologico in cui il passato di ogni individuo possa riemergere con poche o nessuna possibilità di controllo, la sua vita privata possa essere registrata in una sorte di memoria permanente della rete sempre di più somigliante a quella di Funes el Memorioso, personaggio nato dalla fantasia di Borges e oggi quanto mai identificabile non in un individuo dalla memoria prodigiosa ma nell'insieme di strumenti di ricerca e sistemi di memorizzazione, *sharing* di dati o *social networks* disponibili *online* sulla rete. Segnali incoraggianti vengono dallo sviluppo di tecnologie di ricerca di tipo semantico che, oltre a essere più accurate ed efficaci, presuppongono tuttavia modifiche sostanziali alla modalità di presentazione e di elaborazione delle informazioni.

Il successo di qualsiasi iniziativa volta a concretizzare anche in prodotti tecnologici i principi della protezione dei dati dipenderà dalla capacità di affermarli e promuoverli tra la vasta platea costituita dalla comunità di utenti e sviluppatori della rete, in un'era in cui i valori della *privacy* e della protezione dei dati personali vanno incontro a un'altalena di percezioni e considerazioni anche da parte del pubblico, dei legislatori e, più in generale, dei *policy makers*, in un conflittuale rapporto tra libertà di espressione, diritto di conoscere da parte del pubblico e diritto dell'individuo di sottrarsi all'azione invasiva delle tecnologie della rete.

Abstract

This paper describes the fundamental choices available to programmers, software developers and web designers for limiting the spread of data published on a World Wide Web site. Features and limitations of different methods are discussed, together with a brief historical introduction to the notion of infor-

mation indexing related to Internet services, with a special focus on the Robot Exclusion Protocol adopted by web publishers around the Net in order to allow or deny a crawler agent the access to web contents.

The well-known Google Spain case decided by the European Court of Justice in May 2014 is also shortly debated for its implications related to the technical means required for the compliance.

Giovanni Maria Riccio

Diritto all'oblio e responsabilità dei motori di ricerca

SOMMARIO: 1. La responsabilità degli operatori di internet - 2. Le argomentazioni della Corte di Giustizia - 3. Una procedura di *notice and take-down* per i dati personali? - 4. Quali parametri per la rimozione dei risultati della ricerca? - 5. Danno da permanenza nei risultati della ricerca? - 6. Conclusioni

1. La responsabilità degli operatori di Internet

La sentenza della Corte di Giustizia sul diritto all'oblio nei motori di ricerca stimola l'attenzione dell'interprete su molteplici punti di riflessione, che—pur partendo dalla disciplina settoriale della tutela dei dati personali—inevitabilmente abbracciano altri settori dell'ordinamento¹. Se osservata sotto l'immaginaria lente di ingrandimento dello studioso di responsabilità civile, la decisione del maggio scorso solleva complessi interrogativi, determinati dai silenzi della Corte, che riconosce espressamente un diritto soggettivo (nella forma del diritto all'oblio o alla cancellazione) in capo ai cittadini comunitari, ma non delimita gli obblighi cui sono tenuti i motori di ricerca. Una conclusione che potrebbe non solo mutare la relazione tra utenti e reti telematiche, disconoscendo la troppe volte preconizzata morte della *privacy*², ma, verosimilmente, potrebbe determinare un deciso ripensamento del principio della neutralità degli intermediari della rete.

Prima di affrontare nel dettaglio le problematiche sollevate dalla decisione, pare opportuno ripercorrere, seppur in estrema sintesi, i principi che governano la responsabilità civile degli operatori di internet.

Com'è noto, la responsabilità degli ISP (*intermediary service provider*) è disciplinata dalla Sezione 4 della direttiva 2000/31/CE sul commercio

¹ Per un primo tentativo di ricostruzione sistematica delle interrelazioni e delle problematiche giuridiche nel rapporto tra oblio e reti telematiche, v. il volume collettaneo AA.VV., *Il caso del diritto all'oblio*, a cura di F. Pizzetti, Torino, 2013.

² Cfr., *ex multis*, A.M. FROOMKIN, *The Death of Privacy?*, 52 *Stan. L. Rev.* . 1461 (2000), ma ancor prima D.L. ZIMMERMANN, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 *Cornell L. Rev.* p. 291 (1983).

elettronico. La normativa comunitaria è frutto di un processo di circolazione e di imitazione del modello statunitense del § 512 del DMCA³ – ripreso talora pedissequamente nelle formule legislative della direttiva – e del *Teledienstgesetz*, la legge tedesca sulla responsabilità degli intermediari. Rispetto a tali modelli, tuttavia, la direttiva si differenzia per due importanti aspetti: innanzi tutto, l'ambito di applicazione oggettiva abbraccia sia gli illeciti civili sia quelli penali; in secondo luogo, sotto il profilo soggettivo, la disciplina comunitaria non include le attività dei motori di ricerca⁴ e il *linkin*⁵. Allo stesso modo – e questo aspetto rappresenta probabilmente il maggior limite della Sezione 4 sulla responsabilità degli intermediari di internet – non sono previste forme di *notice and take-down* per determinare le modalità per i titolari dei diritti di indirizzare una richiesta di

³ *Digital Millennium Copyright Act* del 1998, che ha riformato il *Copyright Act* del 1976 e ratificato i discussi trattati dell'Organizzazione Mondiale per la Proprietà Intellettuale, WIPO *Copyright Treaty* (WCT) e il WIPO *Performances and Phonograms Treaty* (WPPT). Sul punto, per un quadro di insieme, v. P. SAMUELSON, *The U.S. Digital Agenda at WIPO*, p. 37 *Va. J. Int'l L.* 369 (1997).

⁴ In sede di recepimento della direttiva, alcuni ordinamenti hanno disciplinato però l'attività dei motori di ricerca: così l'art. 17 della *Ley* spagnola che estende le regole per i fornitori di *hosting* ai motori di ricerca; sul punto si rinvia a M. PEGUERA, *Internet Service Providers' Liability in Spain: Recent Case Law and Future Perspective*, 13 *J. of Intell. Prop. Information Tech. and E-Commerce Law* 151 (2010). All'interno della giurisprudenza spagnola, il *leading case* è rappresentato da Tribunale Supremo - Sala Primera, 3 aprile 2012, Alexis Pedragosa Llaurodo c. Google Spain SL, che, in un caso di violazione del *copyright* per riproduzione, da parte di Google, degli *snippet* (miniature di immagini) di altro sito, ha ritenuto che la natura e la funzione dei servizi dei motori di ricerca, che dovrebbero aiutare gli utenti nel reperimento e nella selezione delle informazioni pubblicate in rete, sarebbe incompatibile con le finalità di violazione dei diritti di esclusiva del soggetto attore.

⁵ V. SÉDALLIAN, *La responsabilité des prestataires techniques sur Internet dans le Digital Millennium Copyright Act américain et le projet de directive européen sur le commerce électronique*, in *Cahiers Lamy droit de l'informatique et des réseaux*, 1999, n. 110, p. 1; C. ROJINSKY, *Commerce électronique et responsabilité des acteurs de l'Internet en Europe*, in *Gaz. Pal.*, 23-24 juin 2000, 19; E. MONTERO, *La responsabilité des prestataires intermédiaires de l'Internet*, in *Revue Ubiquité*, 2000, 100; R. JULIÀ-BARCELÓ - K.J. KOELMAN, *Intermediary Liability in the E-Commerce Directive: So Far So Good, But It's Not Enough*, in 16 *Computer Law & Security Report*, p. 231 (2000); A. STROWEL - N. IDE - F. VERHOESTRAETE, *La directive du 8 juin 2000 sur le commerce électronique: un cadre juridique pour l'internet*, in *Jour. des Tribunaux*, 2001, n. 6000, p. 141; F. DI CIOMMO, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, 2003; *passim*; R. BOCCHINI, *La responsabilità civile degli intermediari del commercio elettronico. Contributo allo studio dell'illecito plurisoggettivo permanente*, Napoli, 2003; *passim*; ma sul punto sia consentito rinviare anche G.M. RICCIO, *La responsabilità civile degli internet providers*, Torino, 2002, pp. 200 ss.

rimozione di eventuali contenuti illeciti agli ISP e, dall'altro lato, non è fissato il momento in cui questi ultimi, informati della commissione di un illecito, possono essere tenuti, a determinate circostanze, a rimuovere detti contenuti.

Per quanto attiene all'ambito di applicazione oggettiva, occorre poi ricordare che la direttiva sul commercio elettronico non trova applicazione, *ex art. 1, par. 4, lett. b)*, alle «questioni relative ai servizi della società dell'informazione oggetto delle direttive 95/46/CE e 97/66/CE» e, quindi, a tutto il settore della tutela dei dati personali. Il regime speciale di responsabilità previsto, in generale, per gli ISP, non si estende, pertanto, anche all'attività di trattamento delle informazioni personali che, viceversa, è regolato dall'art. 23 della direttiva 95/46/CE, così come recepito nei singoli ordinamenti nazionali.

Naturalmente, non è questa la sede per ripercorrere i dibattiti dottrinali e giurisprudenziali che hanno condotto all'emanazione della direttiva sul commercio elettronico; ci limiteremo, pertanto, a rammentare i principi che hanno mosso l'operato del legislatore comunitario. Le due colonne sulle quali poggia l'architrave disegnato dalla direttiva sono, in estrema sintesi, il summenzionato principio della neutralità degli operatori, in virtù del quale gli ISP non sono responsabili se la loro attività si limita ad un ruolo tecnico e non selezionano né i contenuti, né i destinatari delle informazioni, e l'assenza di un obbligo generale di sorveglianza sui contenuti diffusi dai destinatari dei propri servizi. La direttiva, quindi, ha optato per un modello di responsabilità fondato sulla colpa degli operatori, considerati come meri *carrier* dei contenuti informativi⁶, scartando le ipotesi di responsabilità oggettiva, come la responsabilità da rischio di impresa o editoriale. Una scelta apprezzata dalla dottrina, che ha consentito lo sviluppo economico dei nuovi operatori e ha scongiurato ogni rischio

⁶ La neutralità dei *common carrier* è stata sostenuta dalla giurisprudenza statunitense ben prima dell'avvento di internet: cfr. *National Ass'n of Regulatory Util. Comm'r's v. FCC*, 533 F.2d 601, 608 (D.C. Cir. 1976), ma v. già, a proposito dell'indifferenza dei fornitori delle infrastrutture ai contenuti, *Western Union Tel. v. Lesesne*, 182 F.2d 135, 137 (5th Cir. 1950). Il criterio applicato dalle corti nordamericane è riassumibile nel *reason to know test*: i *common carrier* sono responsabili se, al momento della diffusione, sono a conoscenza (o avrebbero dovuto esserlo, usando l'ordinaria diligenza) dei contenuti veicolati: cfr. *O'Brien v. Western Union Tel. Co.*, 113 F.2d 539, 542 (1st Cir. 1940). Tale ricostruzione trova applicazione a tutti i casi in cui non vi è selezione dei contenuti da parte del gestore del mezzo di comunicazione: così per il telegrafo (*Western Union Tel. Co. v. Lesesne*, 182 F.2d 135, 137 (4th Cir. 1950); *O'Brien v. Western Union Tel. Co.*, 113 F.2d 539, 542 (1st Cir. 1940)), per il telefono (*Anderson v. New York Tel. Co.*, cit.); per i servizi telefonici automatizzati (*People v. Lauria*, 59 Cal. Rptr. p. 628 (1967)).

di assegnazione di poteri ‘censori’ in capo agli ISP⁷.

A distanza di quasi un quindicennio, lo scenario da cui muoveva la direttiva è però radicalmente mutato. Lo studio dello sviluppo delle imprese della *new economy* ha evidenziato alcune peculiarità rispetto alle imprese tradizionali, tra cui la capacità di realizzare, in un lasso di tempo relativamente breve, posizioni monopolistiche o dominanti sul mercato di riferimento. Allo stesso modo, pur in presenza di costi di *start-up* molto limitati, alcune di queste imprese hanno generato enormi utili, moltiplicando il proprio potere commerciale in pochi anni: non stupisce, quindi, che, scorrendo la classifica dei marchi di maggior valore, ci si avvede che le prime quattro posizioni sono occupate da società che operano prevalentemente nel ‘mondo’ di internet⁸.

In tale contesto, è giocoforza ammettere che gli operatori di internet, pur se agiscono da intermediari, hanno assunto un ruolo di *deep pocket parties*⁹; e, sempre per tale ragione, appare condivisibile la conclusione della Corte di Giustizia, che afferma categoricamente che il riconoscimento di un diritto all’oblio in capo ai singoli cittadini debba prevalere «sull’interesse economico del gestore del motore di ricerca»¹⁰ e che – la sentenza non lo dice espressamente, ma è un corollario ovvio – i motori di ricerca debbano essere chiamati a sopportare i costi sociali finalizzati ad assicurare la piena tutela nel trattamento dei dati personali.

⁷ Sul punto, per ulteriori rilievi, sia consentito rinviare a G.M. RICCIO, *La responsabilità civile degli internet providers*, cit., 202 ss.

⁸ Si fa riferimento alla classifica annuale *BrandZ Top100 most valuable global brands 2014*, che vede, nei primi quattro posti, rispettivamente Google, Apple, IBM e Microsoft. Sorprende, poi, che il marchio Google valga circa il doppio del marchio Coca-Cola e, soprattutto, che il suo valore abbia registrato un incremento, nel solo ultimo anno, del 40%. I dati riportati sono confermati da altre analoghe ricerche, come, ad esempio, quella di *Millward Brown Optimor*.

⁹ Il richiamo è a G. CALABRESI, *Costo degli incidenti e responsabilità civile*, trad. it., Milano, 1975, pp. 65 ss. che osserva come l’esigenza di «ridurre i costi secondari dei sinistri» determini la scelta di trasferirli «su quelle categorie di persone, la cui posizione sociale ed economica meno ne risentirebbe, su quelli, cioè, che generalmente si sogliono definire ‘ricchi’». Ha parlato da tempo di ISP come soggetti con le ‘tasche profonde’ G. PONZANELLI, *Verso un diritto uniforme per la responsabilità degli internet service providers*, in S. SICA - P. STANZIONE, *Commercio elettronico e categorie civilistiche*, Milano, 2002, p. 368.

¹⁰ Conclusioni considerate legittime in uno dei primi commenti alla decisione, cfr. F. PICOD, *Renforcement de la responsabilité de Google et droit au retrait des données personnelles*, in *Semaine Juridique*, n. 21-22, 26 Mai 2014, 629, p. 1068.

2. Le argomentazioni della Corte di Giustizia

Partendo da tale conclusione, occorre, tuttavia, analizzare brevemente il percorso argomentativo della Corte e i presupposti normativi che condurrebbero, nell'interpretazione dei giudici comunitari, all'applicazione della disciplina in materia di *privacy* ai motori di ricerca.

Il punto d'arrivo della decisione è, in astratto, condivisibile: non v'è dubbio, infatti, che i diritti della personalità prevalgano sugli interessi economici degli operatori, così come affermato, in altri contesti, dalla stessa Corte¹¹.

Del pari, sembra corretto sostenere che le attività compiute dai motori di ricerca – reperire contenuti tra i vari siti internet, indicizzarli, memorizzarli temporaneamente (c.d. *caching*) – costituisca un trattamento di dati personali. È discutibile, invece, che il gestore di un motore di ricerca possa essere considerato responsabile (o titolare, se si utilizza la terminologia italiana) del trattamento dei dati personali e che, quindi, possa essere il soggetto «che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali» (art. 2 lett. *d*) direttiva 95/46/CE) pur in presenza di un processo automatizzato di ricerca e di una selezione volontaria dei contenuti (*rectius*: dati personali).

La questione, data la complessità degli argomenti sostenuti, non può che essere accennata: valga la pena però segnalare che la Corte di Giustizia, assimilando la posizione di Google a quella di un titolare del trattamento, ha ribaltato non solo l'opinione dell'Avvocato Generale¹², ma altresì quella

¹¹ Sul punto, per tutti, G. RESTA, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato*, in *Dir. Inf.* 2014, 171.

¹² L'Avvocato Generale aveva sostenuto l'inapplicabilità del ruolo di titolare del trattamento ai motori di ricerca per due essenziali ragioni. La prima risiede nell'attività concretamente svolta: «Il fornitore di servizi di motore di ricerca su Internet che offre semplicemente uno strumento di localizzazione delle informazioni non esercita alcun controllo sui dati personali contenuti in pagine web di terzi. Il fornitore di servizi è «consapevole» dell'esistenza di dati personali unicamente nel senso che, sotto un profilo statistico, è probabile che le pagine web contengano dati personali. Durante il trattamento delle pagine web source a scopo di esplorazione, di analisi e di indicizzazione, i dati personali non si manifestano in quanto tali in alcun modo particolare»; la seconda, invece, sull'inattualità della direttiva e sulla sua incapacità a disciplinare situazioni, come quella in questione, sconosciute al legislatore comunitario del 1995: «Quando la direttiva è stata adottata, il World Wide Web era una realtà appena comparsa e i motori di ricerca su Internet erano ancora agli inizi. Le disposizioni della direttiva semplicemente non tengono conto del fatto che masse ingenti di documenti e di file elettronici ospitati in maniera decentralizzata sono accessibili da qualsiasi parte del mondo e che i loro contenuti possono essere copiati, analizzati e diffusi da persone che non hanno alcuna relazione con i rispettivi

dell'Article 29 Working Party che, nella *Opinion* 1/2008, aveva sostenuto la necessità di una lettura della direttiva «fattuale, piuttosto che formale» con «attribuzione di responsabilità laddove intervenga un'influenza effettiva»¹³. Appare altresì opinabile che la sentenza, adottando un'interpretazione estensiva¹⁴, abbia considerato applicabile il diritto nazionale poiché effettuato «nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro», pur in assenza della prova di un trattamento di dati personali dalla Google Spain, società stabilita in Spagna e controllata dalla società madre Google Inc., che gestisce autonomamente i server e realizza indipendentemente l'attività di memorizzazione¹⁵.

Anche su tale aspetto, l'Article 29 Working Party aveva manifestato un'opinione antitetica, concludendo che, ai fini dell'applicazione della legge nazionale, lo stabilimento del responsabile del trattamento dovrebbe realizzare «attività che comportano il trattamento di dati personali, tenendo conto del suo livello di partecipazione alle attività di trattamento, della

autori o con quanti li hanno caricati in un server host connesso a Internet». La Corte di Giustizia, già nel caso *Lindqvist* (6 novembre 2003, C-101/01, *Racc.*, 2003 p. I-12971) aveva adottato un'interpretazione della direttiva adeguandola al mutato scenario tecnologico, ritenendo che, in caso di trasferimento dei dati personali via internet, non fossero applicabili all'uso di Internet i criteri elencati nella direttiva.

¹³ Il parere citato è disponibile sulla pagina dell'Article 29 Working Party all'URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf [consultato il 30/09/2014].

¹⁴ Cfr. il punto 53 della sentenza: «alla luce dell'obiettivo della direttiva 95/46 di garantire una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, con riguardo al trattamento dei dati personali, l'espressione suddetta (nel contesto delle attività di uno stabilimento, n.d.r.) non può ricevere un'interpretazione restrittiva».

¹⁵ Deve, tuttavia, ammettersi che le diverse corti europee hanno sempre tentato di esercitare una sorta di *vis attractiva*, ammettendo la propria giurisdizione ovvero l'applicabilità della propria legge nazionale; merita di essere ricordata, da ultima, la decisione dell'Oberlandesgericht des Landes Berlin del 24 gennaio 2014, che ha ritenuto invalida l'informativa prestata agli utenti tedeschi (*Datenschutzrichtlinien*) da Facebook, che applicava il diritto statunitense, pur effettuando, a giudizio della Corte, un trattamento di dati personali nel territorio tedesco. La decisione in questione è interessante, anche perché ribalta un precedente della Schleswig-Holstein Verwaltungsgericht del 14 febbraio 2013, che aveva negato l'applicabilità della normativa tedesca ai *social network* i cui server sono localizzati negli Stati Uniti. Le decisioni sono disponibili rispettivamente agli URL <http://www.berlin.de/sen/justiz/gerichte/kg/presse/archiv/20140214.1835.394435.html> [consultato il 30/09/2014] e <https://www.datenschutzzentrum.de/facebook/Facebook-Ireland-vs-ULD-Beschluss.pdf> [consultato il 30/09/2014]. Cfr. anche Bundesgerichtshof, 14/05/2013, in *Dir.Inf.*, 2013, p. 541, con nota di G. GIANNONE CODIGLIONE, cui si rinvia per ulteriori richiami di dottrina e giurisprudenza.

natura delle attività e della necessità di garantire un'effettiva protezione dei dati». In altri termini, non dovrebbe essere sufficiente il collegamento economico tra la *parent company* (Google Inc., nella fattispecie che ci interessa) e la società controllata (Google Spain), richiedendosi un coinvolgimento effettivo di quest'ultima nelle scelte relative al trattamento realizzato¹⁶.

L'opzione argomentativa prescelta si presta, come qualche commentatore ha già osservato, a facili elusioni: sarebbe, infatti, sufficiente, per aggirare l'*iter* argomentativo della Corte di Giustizia, che i servizi accessori – come quelli pubblicitari del caso di specie – siano commercializzati da un soggetto terzo, non controllato dalla Google Inc., ma alla stessa legato da un rapporto di consulenza¹⁷. La soluzione offerta, peraltro, anticipa quelli che potrebbero essere gli effetti dell'adozione Regolamento in materia di dati personali, la cui proposta, all'art. 3, par. 2, recepisce il c.d. *target principle*¹⁸, estendendo l'applicazione territoriale anche ai soggetti stabiliti fuori dall'Unione europea, laddove gli stessi offrano beni o servizi ai residenti nell'Unione ovvero controllino il loro comportamento (espressione talmente generica da ricomprendere attività disomogenee e amplissime)¹⁹. La normativa europea, quindi, si sta instrandando – e la sentenza in commento sembra collocarsi in tale solco – verso l'applicazione universale del diritto comunitario²⁰, determinando conseguenze difficili da prevedere nella loro entità, ma che condurranno inevitabilmente ad una frizione nei

¹⁶ Anche la localizzazione dei dispositivi per ottenere i dati personali è un aspetto fondamentale che, a parere di chi scrive, non consente di assimilare il caso in questione con quello di *Street View*, su cui v. il provvedimento del 15 ottobre 2010 del Garante per la tutela dei dati personali che, correttamente, ha affermato l'applicabilità del diritto nazionale, sul punto v. L. MONTUORI, *Applicabilità della normativa comunitaria e italiana. una questione interpretativa*, in *Sicurezza e Giustizia*, 2013, p. 32, nota 10.

¹⁷ G. SCORZA, *Corte di Giustizia e diritto all'oblio: una sentenza che non convince*, in *Corr. giuridico*, 2014, in corso di pubblicazione; *contra* L. MONTUORI, *op. cit.*, pp. 30 ss.

¹⁸ Cfr. M. CARTA, *Diritto alla vita privata ed internet nell'esperienza giuridica europea ed internazionale*, in *Dir.Inf.*, 2013, p. 17.

¹⁹ Non a caso la Commissione competente del Parlamento europeo (Libe – Libertà civili, giustizia e affari interni), nel votare il 21 ottobre 2013 gli emendamenti alla proposta di direttiva (cfr. Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 - C7 0025/2012 - 2012/0011(COD)) Compromise amendments on Articles 1-29) ha proposto di sostituire la formulazione «the monitoring of their behaviour» con «the monitoring of such data subjects».

²⁰ L'applicazione universale della normativa sul trattamento dei dati personali era uno degli effetti da scongiurare, secondo il già ricordato parere del *Working Group*.

rapporti, politici e commerciali, tra Europa e Stati Uniti²¹. Né può dirsi nuova la progressiva tendenza della Corte di Giustizia ad anticipare o a contraddire, a seconda dei casi, le posizioni della Commissione, determinando, di fatto, una pericolosa invasione di poteri, opportunamente segnalata dalla dottrina più attenta²².

3. Una procedura di 'notice and take down' per i dati personali?

A seguito della sentenza, Google ha introdotto sui propri siti europei un modulo per la rimozione di risultati di ricerca²³. Per mezzo di tale modulo gli utenti – anche per il tramite di un proprio rappresentante (genitore, avvocato, e così via enumerando) – possono richiedere che siano rimossi i risultati connessi ad un determinato nome. Lo scopo principale di tale sistema – al pari degli altri esempi di *self-regulation* da tempo adottati dagli ISP – è quello di ridurre i costi transattivi, predisponendo formulari di pronta consultazione, che consentano un'analisi rapida dei

²¹ Come previsto già da L. BYGRAVE, *Determining Applicable Law Pursuant to European Data Protection Legislation*, 16 *Computer L. & Sec. Rev.* 252, p. 254 (2000). La questione è ampiamente discussa da D.J.B. SVANTESSON, *The Extraterritoriality of Eu Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, *Stanford J. of Int'l Law* 53 (2013), pp. 94-102, che suggerisce l'elaborazione di una *market sovereignty doctrine* per la risoluzione delle controversie relative alla giurisdizione e alla legge applicabile su internet. Lo stesso A. evidenzia una possibile applicazione paradossale della regola fissata nell'art. 3 della proposta di direttiva: poiché la norma fa riferimento al concetto di residenza, essa troverebbe applicazione anche ai turisti comunitari che ricevono un servizio trovandosi, temporaneamente, negli Stati Uniti o in un altro Stato extra-UE.

²² Cfr., all'interno di una copiosa bibliografia, G. DE BURCA - J.H.H. WEILER, *The Worlds of European Constitutionalism*, Cambridge, 2011 (in particolare il capitol di G. DE BURCA, *The ECJ and the international legal order: a re-evaluation*); nonché, più recentemente, M. DAWSON - B. DE WITTE - E. MUIR, *Judicial Activism At The European Court Of Justice*, Londra, 2013. Come accennato nel testo, sono tutt'altro che rari i casi di scontro, più o meno dichiarato, tra istituzioni comunitarie; v. di recente la decisione OSA del 27 febbraio 2014 (causa C-351/12): per ulteriori rilievi sul punto, si rinvia a J. DREXL, *Collective Management of Copyrights and the EU Principle of Free Movement of Services after the Osa Judgment - In Favour of a More Balanced Approach*, Max Planck Institute for Innovation and Competition Research Paper No. 14-06, München, 2014, ma sia consentito altresì richiamare G.M. RICCIO, *Gestione collettiva dei diritti d'autore: all'alba di uno scontro tra istituzioni comunitarie?*, in corso di pubblicazione in *Nuova giur. civ. comm.*, 2014.

²³ https://support.google.com/legal/contact/lr_eudpa?product=websearch [consultato il 30/09/2014].

casi da trattare, evitando costi giudiziali. Si pensi a quanto avviene con le violazioni della proprietà intellettuale: molti operatori di internet hanno predisposto dei meccanismi di *private enforcement* per mezzo dei quali rimuovono i contenuti una volta ricevuta una segnalazione da parte di un utente (basti ricordare, per citare esempi noti, al *VeRo Program* di eBay²⁴, al programma *Content ID* di YouTube e alla procedura di segnalazioni di *trademark infringements* di Facebook)²⁵. Di là da tali esempi di autoregolamentazione, l'esperienza più significativa è rappresentata dalla procedura di *notice and takedown* disciplinata, in materia di diritto d'autore, dal § 512 (c) (3) (A) del DMCA. Una procedura che, come si è detto, non è stata ripresa dal legislatore comunitario, ma che ha subito un processo singolare di circolazione giuridica: in alcuni Stati europei (ad esempio, in Finlandia, Lituania e Ungheria) sono state introdotte procedure analoghe, basate sull'imitazione del modello statunitense²⁶.

Le differenze principali tra il modello predisposto da Google e da altri motori di ricerca²⁷ per la deindicizzazione dei contenuti e la procedura di notifica e rimozione, prevista nei casi di violazioni del diritto d'autore, sono essenzialmente due. In primo luogo, la *notice and take-down* in materia di copyright trova la propria fonte in un testo normativo, il § 512 (c) (3) (A) del DMCA²⁸. In secondo luogo, il DMCA prevede una

²⁴ Il *Vero Program* è un accordo che «consente ai titolari di un diritto di proprietà intellettuale (come copyright, marchi registrati o brevetti) di segnalare le inserzioni che ne violano la proprietà intellettuale». In altri termini, si tratta di un accordo contrattuale per mezzo del quale eBay si impegna a rimuovere le aste telematiche presenti all'interno della propria piattaforma una volta ricevuta una segnalazione dai soggetti autenticati, che hanno aderito al *VeRo Program*. In questo, come negli altri casi menzionati nel testo, le condizioni generali di contratto ammettono che il gestore della piattaforma possa rimuovere i contenuti pubblicati dagli utenti, senza incorrere in alcuna responsabilità. Sul rapporto dominante che esercitano i gestori dei *social network* e, più in generale, gli operatori del web 2.0, si rinvia a R. CATERINA, *Cyberspazio, social network e teoria generale del contratto*, in *AIDA*, 2011, pp. 93 ss.

²⁵ Sul punto sia consentito rinviare a G.M. RICCIO, *Old Economy v. New Economy: Intellectual Property, Global Wrongs and Private Remedies*, in *Virtualis* 2013, pp. 131 ss.

²⁶ La soluzione adottata è stata inoltre suggerita dal gruppo di esperti nominati alla Commissione europea in sede di revisione della sezione 4 della direttiva sul commercio elettronico: cfr. T. VERBIEST - G. SPINDLER - G.M. RICCIO - A. VAN DER PERRE, *Study on the Liability of Internet Intermediaries*, Markt 2006/09/E, DG Internal Market, Bruxelles, November 2007, p.p 15 ss. e pp. 106 ss.

²⁷ Al momento, per quanto è dato sapere, solo Bing si è dotata di un modello di richiesta per la rimozione dei collegamenti ipertestuali: cfr. J. VINCENT, *Bing implements 'right to be forgotten' ruling, asks applicants 'are you famous?'*, *The Independent*, Thursday 17 July 2014.

²⁸ La *notification* deve contenere i seguenti requisiti: la sottoscrizione, fisica o elettronica,

forma di difesa in capo al soggetto che ha pubblicato il contenuto che si afferma aver violato un diritto di proprietà intellettuale: tale soggetto, una volta ricevuta la copia della *notification* inoltratagli dall'ISP, ha la possibilità di indirizzare una *counter-notification*, che deve contenere i medesimi requisiti della contestazione e le ragioni per cui i contenuti segnalati non dovrebbero essere rimossi (es. esistenza di una licenza che legittimi la distribuzione).

Google, infatti, si limita a comunicare al soggetto che ha pubblicato il contenuto di aver rimosso il *link*, ma non consente a tale soggetto di replicare, eccependo la sussistenza di una delle «ragioni particolari» succintamente evocate dalla Corte. L'editore del contenuto, per riottenere l'indicizzazione della notizia, sarà quindi costretto ad agire dinanzi all'Autorità giudiziaria ovvero al Garante per la protezione dei dati personali competente per territorio. In definitiva, nel caso del modello previsto per il diritto all'oblio, siamo al cospetto di un modulo, finalizzato alla prevenzione di azioni giudiziarie da parte di terzi, che non è normativamente disciplinato né imposto dalla pronuncia della Corte di Giustizia.

Si tratta di un mezzo privato di autodisciplina – e che dei limiti dell'autodisciplina è esempio – attraverso il quale i motori di ricerca tentano di dare soluzione agli effetti della sentenza che ci interessa²⁹. A prescindere da tale profilo, di per sé di estrema importanza, pare necessario interrogarsi sulle prassi che Google e gli altri motori di ricerca adotteranno per la rimozione delle pagine segnalate.

L'esperienza in materia di *copyright* induce ad essere cauti e a sollevare talune inquietudini, seppur al momento meramente potenziali. Nel caso in cui si segnalino contenuti che si assume violino i propri diritti d'autore (ovvero altri diritti di proprietà intellettuale), Google rimuove automati-

del soggetto che promuove l'istanza; l'identificazione dell'opera sulla quale il promotore dell'istanza vanta (o, almeno, dichiara di vantare) uno o più diritti esclusivi, violati dalla diffusione in Rete; l'identificazione del materiale diffuso che viola questi diritti e di cui si chiede la rimozione o il blocco dell'accesso; un indirizzo, un numero di telefono e, se disponibile, un *e-mail*, che consentano di contattare il soggetto che ha promosso l'istanza; una dichiarazione resa da quest'ultimo, nella quale si attesta che la *complaining party* ritiene, in buona fede, che la diffusione del materiale non sia autorizzata dal titolare del copyright, da un suo *agent* o dalla legge; una dichiarazione nella quale si attesta che la notificazione è completa e che il soggetto che la propone agisce per conto del titolare del diritto violato.

²⁹ Cfr. G. GIANNONE CODIGLIONE, *Motori di ricerca, trattamento di dati personali ed obbligo di rimozione: diritto all'oblio o all'autodeterminazione informativa?*, in *Nuova giur. civ. comm.*, in corso di pubblicazione.

camente detti contenuti dai propri servizi (es. YouTube)³⁰, limitandosi poi a pubblicare un avviso nel quale menziona che la rimozione è avvenuta a seguito della *notification* ricevuta da un determinato utente³¹. Ciò ha determinato che, sovente, il ricorso al sistema di *Content ID* sia avvenuto anche nel caso di violazione di altri diritti: si pensi, ad esempio, alla possibilità di chiedere la rimozione in caso di contenuti diffamatori, al fine di aggirare le strettoie poste dal *Communications Decency Act* che, di fatto, legittima gli ISP a non attivarsi per la soppressione dei contenuti illeciti, anche laddove siano informati dai titolari dei relativi diritti³².

La soluzione, del resto, è l'unica rispettosa del principio di neutralità degli operatori, enunciato dal DMCA e, successivamente, dalla direttiva sul commercio elettronico: gli ISP rimuovono i contenuti senza interrogarsi sulla loro liceità, non essendo tenuti ad operare alcun controllo; agiscono da meri intermediari, informando i soggetti che hanno 'caricato' i contenuti (cc.dd. *uploaders*) dell'avvenuta rimozione; inoltrano a tali soggetti la *notification*, mettendoli, eventualmente, in condizione di replicare³³. È ipotizzabile che una simile strada sarà intrapresa anche nei casi di segnalazione dei risultati della ricerca? Che, quindi, Google e gli altri motori di ricerca si limiteranno ad eliminare i collegamenti, senza interrogarsi sull'eventuale sussistenza di ragioni preponderanti di interesse pubblico³⁴?

³⁰ In questo senso, Google si distingue rispetto ad altri operatori.

³¹ Nel momento in cui si scrive (luglio 2014) 25.184.774 video sono stati rimossi da YouTube dal 2007. La piattaforma non pubblica i dati relativi alle *notification* che non hanno determinato la rimozione del video, limitandosi a menzionare taluni video. Ciò rende, di fatto, impossibile calcolare la percentuale di video rimossi rispetto alle richieste avanzate dai titolari dei diritti.

³² Si ricorda che la § 230 (c) (1) («Treatment of Publisher or Speaker») dispone che nessun fornitore o utilizzatore di un servizio interattivo telematico può essere trattato alla stregua di un editore nei confronti delle informazioni offerte da un altro fornitore di contenuto. Ciò ha determinato, nei fatti, una assoluta irresponsabilità degli ISP, come hanno dimostrato, immediatamente dopo l'adozione della norma, i casi *Zeran v. AOL*, 958 F. Supp. 1124, (E.D. Va. 1997), *aff'd* 129 F.3d 327, (4th Cir. 1997), *cert. denied* 118 S. Ct. 2341(1998) e *Lunney v. Prodigy Services*, 683 N.Y.S. 2d 557 (App. Div. 1998), *aff'd* 164, 1999 N.Y. Lexis 3746 (1999).

³³ Cfr., da ultimo, F. RESTA, *La rete e le utopie regressive (sulla conclusione del caso Google/Vividown)*, in *Dir. Inf.* 2014, 240-241: «il "sistema di 'notice and take down' – centrale nella direttiva sul commercio elettronico – a garantire al punto più alto l'equilibrio tra libertà e responsabilità in rete; tra libertà di espressione e difesa dei diritti delle vittime dei reati commessi on-line; tra assenza di censure e doveroso accertamento delle responsabilità di chiunque abbia usato la rete per offendere, ingiuriare, ledere gli altrui diritti e libertà"».

³⁴ Il medesimo quesito è posto anche da A. PALMIERI - R. PARDOLESI, *Dal diritto all'oblio*

Pur senza voler indulgere in facili catastrofismi o paventare chilling effect o SLAPP (strategy law against public participation)³⁵, è un rischio, a parere di chi scrive, più che probabile, per una molteplicità di ragioni. Innanzi tutto, i motori di ricerca tenderanno a ridurre la propria esposizione al pericolo³⁶. Si è detto, infatti, che gli operatori si limitano a rimuovere il collegamento ipertestuale. Google ha dichiarato di comunicare l'avvenuta procedura agli uploader, sebbene tale obbligo non sia imposto né dalla Corte di Giustizia, né da altra norma; è astrattamente ipotizzabile, nel caso in cui altri operatori adottino una via differente, che l'editore del contenuto non sia informato e si avveda della rimozione solo nel momento in cui effettua una ricerca utilizzando come parola chiave quella del soggetto che ha presentato l'istanza al motore di ricerca. Se si prova ad effettuare un giudizio prognostico sui comportamenti dei soggetti coinvolti, pare lecito supporre che, in caso di omessa rimozione, il segnalante si attiverà per ottenerla dall'Autorità amministrativa per la *privacy* ovvero dall'Autorità giudiziaria.

Naturalmente, nel caso in cui fosse appurata la sussistenza di un diritto all'oblio (*rectius*: alla cancellazione del dato), il gestore del motore di ricerca potrebbe essere chiamato a rispondere sia in qualità di titolare, per illecito trattamento di dati personali, sia, nel caso in cui si ritenga che la permanenza di informazioni relative alla vita privata costituisca un'autonoma voce di danno, a titolo di illecito aquiliano³⁷. Al contrario, se si

all'occultamento in rete: traversie dell'informazione ai tempi di Google, in *Nuovi Quaderni del Foro italiano*, 1/2014, 3: «Siffatta pressione, e il rischio di conseguenti strascichi dinanzi garanti nazionali, potrebbero indurre il provider a rispondere positivamente a tutti, spezzando in maniera indiscriminata il link con la fonte del dato sgradito, senza nemmeno esercitare quel minimo bilanciamento che la Corte di giustizia ammette per le personalità di spicco. O forse spingerà, come pure si vocifera (col probabile intento di innescare un'ondata di esecrazione per il pericolo di oscuramento dell'informazione), a mettere a disposizione di chiunque un apposito 'online tool' da utilizzare per la rimozione dei propri dati dalla ricerca».

³⁵ Sul concetto di SLAPP si rinvia a G. PRING - P. CANAN, *Slapps: Getting Sued for Speaking Out*, Philadelphia, 1996.

³⁶ Il riferimento è, evidentemente, a M. COMPORTI, *Esposizione al pericolo e responsabilità civile*, Napoli, 1965.

³⁷ In passato, la giurisprudenza di merito (Trib. Roma, 20 novembre 1996, in *Dir. inf.*, 1997, 335) ha espressamente affermato che «La riproduzione di vicende attinenti alla vita privata del condannato è suscettibile di produrre un danno ingiusto al diritto all'oblio dei familiari in difetto di un interesse pubblico attuale alla conoscenza di tali vicende». Più recentemente, la giurisprudenza francese ha riconosciuto un danno, a favore di un utente e nei confronti di Google, per la omessa deindicizzazione di un risultato della ricerca; cfr. TGI Parigi, ord., 15 febbraio 2012: «Attendu la société Google Inc., en ne procédant

prova ad immaginare il comportamento dell'editore di un contenuto—a prescindere se il contenuto stesso sia creato e diffuso a titolo professionale o amatoriale — appare poco verosimile che tale soggetto agisca innanzi all'autorità competente, amministrativa o giudiziaria, per ottenere l'indicizzazione delle proprie informazioni. Troppo alti, infatti, appaiono i costi transattivi e troppo blandi (e comunque sbilanciati a favore dell'utente) gli interessi in gioco. Alla luce di tali premesse, se consideriamo il ruolo dei gestori dei motori di ricerca, è facile sostenere che sia economicamente più efficiente 'accontentare' tutti i segnalanti, piuttosto che valutare analiticamente i presupposti di ogni singola segnalazione. Ciò potrebbe condurre verso un fenomeno, ben noto agli studiosi di responsabilità civile, di *over-deterrence*, che dovrebbe spingere gli operatori intermediari ad optare per la soluzione meno rischiosa (ossia la rimozione dei risultati della ricerca), a prescindere dalla sussistenza o meno di un reale diritto all'oblio e alla mancata compresenza di cause che giustifichino la permanenza dell'informazione in rete. Si potrebbe, al più, ipotizzare che l'editore del contenuto faccia leva su di una forma di *moral suasion*, evidenziando le incongruenze e i paradossi conseguenti alla decisione della Corte: tuttavia — e pur prescindendo dal fatto che si tratta di rilievo extra-giuridico, che non elide in alcun modo l'eventuale responsabilità del motore di ricerca — una simile pressione sarebbe esercitabile solo da soggetti dotati di ampia visibilità mediatica, in grado di 'convincere' i motori di ricerca a ripristinare i collegamenti disabilitati, pur in presenza di ragioni di interesse informativo³⁸.

Volendo semplificare, peraltro, ci si potrebbe limitare ad osservare che, seguendo la ricostruzione della sentenza, il soggetto interessato è titolare di un diritto assoluto alla cancellazione del dato personale, mentre un analogo diritto alla indicizzazione dei propri contenuti non è riconosciuto a livello normativo³⁹. Il gestore del motore di ricerca, quindi, difficilmente

pas à la désindexation sollicitée par Madame Z., a participé à la réalisation du dommage moral qu'elle subit du fait que son nom patronymique et son prénom soient associés à des sites pornographiques; que par suite, l'obligation de la société Google Inc. d'indemniser la demanderesse n'est pas sérieusement contestable à hauteur de la somme de 2000 E».

³⁸ Quanto riportato nel testo è già avvenuto nel caso di sei articoli del Guardian, inizialmente rimossi da Google. A seguito delle proteste del quotidiano britannico, il motore di ricerca ha reinserito i collegamenti omessi; cfr. J. BALL, *Google admits to errors over Guardian 'right to be forgotten' link deletions*, *The Guardian*, 10 luglio 2014.

³⁹ Cfr. G. SCORZA, *Corte di Giustizia e diritto all'oblio: una sentenza che non convince*, cit., che correttamente osserva che «il singolo viene a ritrovarsi, dinanzi al trattamento dei propri dati personali svolto dal gestore di un motore di ricerca, titolare di un diritto, pressoché assoluto, alla cancellazione dei propri dati», mentre «nessuno può dirsi titolare di un diritto soggettivo all'indicizzazione, azionabile in qualsivoglia sede e, conseguente-

potrebbe essere chiamato a risarcire un presunto danno da mancata indicizzazione, non gravando sullo stesso – soggetto privato – un dovere di rendere disponibili tutte le informazioni presenti in internet.

I motori di ricerca potrebbero, però, preferire un approccio differente, rigettando la maggior parte delle richieste, al fine di oberare le autorità garanti nazionali, verosimilmente impreparate a gestire centinaia di ricorsi. Ciò determinerebbe due possibili conseguenze: da un lato, sollevare la questione ‘politica’ dell’impossibilità di attuare una tutela efficace; dall’altro, riservare ai *search engine* la selezione dei criteri da adottare per la scelta dei collegamenti da rimuovere.

C’è poi un altro tema, del quale forse si è discusso poco sinora. Le misure conseguenti all’attuazione della sentenza troveranno applicazione solo ai motori di ricerca stabiliti in Europa: ciò potrebbe determinare un vantaggio competitivo per gli operatori extra-europei (ad esempio, Baidu in Cina, che detiene il 17% del mercato mondiale, o Yandex in Russia) che indicizzeranno un numero maggiore di informazioni e, essendo accessibili anche dall’Europa, potrebbero attrarre gli utilizzatori, a scapito dei loro concorrenti⁴⁰. Lo scenario verso il quale si ci potrebbe orientare determinerà, quindi, da un lato, una quantità di informazioni accessibili differente, a seconda del luogo nel quale avviene la ricerca (i contenuti non indicizzati in Europa continueranno ad esserlo fuori dal territorio comunitario), e, dall’altro, consentirà agli operatori, a seconda del luogo nel quale sono stabiliti (luogo che non incide, naturalmente, sulle possibilità di accesso e di utilizzo degli utenti), di offrire contenuti diversi.

4. Quali parametri per la rimozione dei risultati della ricerca?

Un limite della sentenza che ci interessa è rappresentato, peraltro, dall’assenza di parametri chiari da seguire⁴¹. Nell’ultimo paragrafo della

mente, contestare al gestore l’avvenuta disindicizzazione».

⁴⁰ Cfr. L. CHIOU - C. TUCKER, *Search Engines and Data Retention: Implications for Privacy and Antitrust*, MIT Sloan Research Paper, No. 5094-14, i quali notano che alcuni motori di ricerca (es. Yahoo) avevano inizialmente ridotto il tempo di permanenza dei risultati della ricerca, salvo poi ritornare sui propri passi, al fine di essere competitivi nei confronti dei propri concorrenti.

⁴¹ Al contrario, il Garante per la protezione dei dati personali, nel provvedimento dell’11 dicembre 2008, aveva stabilito che gli archivi dei quotidiani dovessero predisporre una versione dell’articolo che non riportasse i dati personali, nel caso in cui l’articolo possa essere estratto automaticamente da motori di ricerca pubblici, e dovessero garantire che le

decisione, la Corte di Giustizia si limita ad affermare che il diritto del singolo non dovrebbe prevalere su quello della collettività ad accedere all'informazione «qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata nell'interesse preponderante del pubblico ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi». È tutt'altro che agevole tradurre, sul piano operativo, quest'affermazione. Il primo presupposto, per preservare la presenza del collegamento ipertestuale, è il tempo. Ma si tratta, evidentemente, di un parametro difficilmente determinabile e, soprattutto, che non può valere per tutte le fattispecie. Il verificarsi di un nuovo accadimento, connesso al precedente per cui si invoca l'oblio, comporta nuovamente attualità dell'informazione⁴²; determinati accadimenti cadono più facilmente nei silenzi della memoria, mentre altri colpiscono indefettibilmente l'immaginario collettivo, generando una loro persistenza tra i primi risultati delle ricerche⁴³.

A prescindere da ciò, è tuttavia probabile che gli operatori di internet, nello scegliere le priorità di intervento e le segnalazioni da smaltire, terranno conto inizialmente di tale elemento, rimuovendo prima i collegamenti più remoti. Il secondo parametro individuato dalla Corte fa riferimento al ruolo ricoperto dal soggetto nella vita pubblica. Si tratta, ancora una volta, di un'affermazione (forse necessariamente) generica, che però non tiene conto delle modifiche che internet ha realizzato sul piano sociale. Da decenni si discute dell'affievolimento della dimensione dicotomica pubblico/privato: con la diffusione dei nuovi media e la parcellizzazione dei canali di comunicazione (social network, televisioni satellitari, ecc.) quali sono le figure pubbliche? Una persona che non ha accesso ai canali televisivi o alla carta stampata, ma che ha diecimila *follower* su Twitter, acquista il rango di figura pubblica⁴⁴? L'analisi degli ordinamenti conti-

notizie siano rintracciabili soltanto usando il motore di ricerca del giornale o del sito web.

⁴² Così, da ultimo, nella giurisprudenza italiana Cass. civ., 26 giugno 2013, n. 16111, in *Danno e resp.*, 2014, p. 271. Nella fattispecie, relativa alle vicende di un terrorista, la Suprema Corte ha statuito che l'oblio non possa essere invocato in presenza di un interesse effettivo ed attuale alla diffusione di una notizia datata, nel senso che quanto recentemente accaduto trovi diretto collegamento con quelle vicende stesse e ne rinnovi l'attualità, diversamente risolvendosi il pubblico ed improprio collegamento tra le due informazioni in un'illegittima lesione del diritto alla riservatezza.

⁴³ Osserva correttamente che l'interesse pubblico non corrisponde però all'interesse del pubblico A. MANTELERO, *Il diritto all'oblio dalla carta stampata ad Internet*, in AA.VV., *Il caso del diritto all'oblio*, cit., p. 152.

⁴⁴ La questione è ampiamente discussa da M. LAFFERMAN, *Do Facebook and Twitter Make*

mentali denota che i confini della nozione di *public figure* sono meno marcati rispetto quelli stabiliti dall'evoluzione analitica della giurisprudenza nordamericana, a partire dai *leading case* *New York Times*⁴⁵ e *Gertz*⁴⁶.

Tuttavia, ancora prima di interrogarsi sulla possibilità di estendere i parametri individuati dalla Supreme Court casi anche agli ordinamenti europei, resta il dubbio che i criteri discretivi possano rimanere immutati al cospetto del mutato scenario dei mezzi di comunicazione di massa. Ha ancora senso sostenere – come nella sentenza *Gertz* – che le figure pubbliche sono quelle che possono avere accesso ai canali di comunicazione⁴⁷ ovvero coloro che – come affermò uno dei ‘padri fondatori’ della *privacy*, il giudice Warren, nel caso *Curtis Publ’g Co.* – possono influenzare il dibattito pubblico e bilanciare, con la propria opinione, le critiche espresse da altri?⁴⁸ Bisogna avvertire, d’altro canto, che anche il tentativo di individuazione case-by-case della natura pubblica del ruolo rivestito dal soggetto interessato è un rischio da scongiurare⁴⁹, giacché ingenererebbe un’incertezza assoluta, probabilmente acuita da differenti indirizzi pretori maturati nei singoli ordinamenti comunitari. Un ultimo dubbio: chi è legittimato a proporre una richiesta di rimozione? Solo il soggetto menzionato nel corpo della notizia o anche colui che è menzionato negli eventuali commenti? Nel silenzio della Corte, non può che darsi risposta affermativa al quesito, considerando che, se i commenti sono indicizzati dal motore di ricerca, si è comunque al cospetto di un trattamento di dati personali.

Le questioni evidenziate, in linea teorica, sollevano affascinanti suggestioni. Tuttavia, come si osservava in precedenza, è fortemente improbabile che i gestori dei motori di ricerca vorranno sobbarcarsi l’ingrato (nonché costoso e rischioso) compito di operare un esame minuzioso di ogni singolo caso: una conclusione avvalorata dallo spropositato numero di segnalazioni – Google, in meno di due mesi dalla sentenza della Corte di Giustizia, ne avrebbe ricevute settantamila per circa duecentocinquantomila pagine web⁵⁰ – e dalla necessità di ridurre i costi transattivi connessi

You a Public Figure?: How to Apply the Gertz Public Figure Doctrine to Social Media, 29 *Santa Clara Computer & High Tech. L.J.* 199 (2012).

⁴⁵ *N.Y. Times Co. v. Sullivan*, 376 U.S. 254 (1964).

⁴⁶ *Gertz v. Robert Welch, Inc.*, 418 U.S. 323 (1974). Sulle due sentenze si rinvia al lavoro, datato, ma pur sempre valido, di V. ZENO-ZENCOVICH, *Onore e reputazione nel sistema del diritto civile*, Napoli, 1985, *passim*.

⁴⁷ *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 344 (1974).

⁴⁸ *Curtis Publ’g Co.*, 388 U.S. 130, 164 (1967) (Warren, C.J., concurring).

⁴⁹ Cfr. D.B. MCKECHNIE, *The Death of the Public Figure Doctrine: How the Internet and the Westboro Baptist Church Spawned a Killer*, 64 *Hastings L.J.* pp. 469, 486-488 (2013).

⁵⁰ Cfr. D. DRUMMOND, *We need to talk about the right to be forgotten*, *The Guardian*,

con l'analisi di tutte le fattispecie.

Il tentativo di prevedere i parametri che saranno adottati dai motori di ricerca nel momento in cui processeranno le richieste degli utenti, ci riporta, inevitabilmente, al punto di arrivo poc'anzi paventato: assecondare le richieste dei segnalanti, prescindendo dalla loro fondatezza, risulta in ogni caso la soluzione più semplice ed economica, nonché quella che espone gli operatori di internet ai minori rischi di essere destinatari di azioni risarcitorie, per aver omesso di intervenire, pur in presenza di legittimi presupposti.

Una conclusione, invero, poco democratica, che finirebbe per assegnare una giustificazione giuridica alla prassi, praticabile da chi ha capacità patrimoniali o nozioni informatiche, di 'sartorializzare' le proprie informazioni personali presenti in rete: basti riflettere sulla possibilità tecnica di modificare i suggerimenti di ricerca (ad esempio il servizio *autocomplete* offerto da Google) ovvero di determinare il posizionamento dei risultati della ricerca inerenti la propria persona. Un ulteriore parametro adottato dai motori di ricerca nella gestione delle segnalazioni potrebbe riguardare la fonte dell'informazione. Le notizie pubblicate sui mezzi di informazione, per dir così, tradizionali (ad esempio, le versioni on-line dei quotidiani cartacei) potrebbero essere considerate come rispondenti ad un interesse pubblico; lo stesso metro di giudizio, invece, potrebbe non essere utilizzato per i cc.dd. *netizen*, ossia coloro che svolgono attività di informazione a titolo non professionale.

È ancora possibile attribuire una 'patente' di attendibilità al *mainstream* sacrificando l'informazione che muove dal basso e la contro-narrazione, spesso antitetica alla narrazione dei media tradizionali, degli accadimenti sociali⁵¹? Come non giudicare un esercizio di schizofrenia l'avvento, da un lato, di un processo di trasmissione dell'informazione *bottom up* e non più *top down*, con tentativi di estendere tutele e garanzie, riconosciute ai giornalisti, anche a *blogger* o semplici cittadini che condividono immagini e video e, dall'altro, il legittimare una diversa durata alla 'vita' delle informazioni, ammettendo che quelle prodotte dai canali dell'informazione tradizionale possano permanere più a lungo nelle reti telematiche? Allo stesso

Thursday 10 July 2014.

⁵¹ È significativo, ad esempio, che, per la riforma del Codice deontologico dei giornalisti (avviata con provvedimento n. 376 del 1 agosto 2013), il Garante abbia invitato alla consultazione anche i rappresentanti dell'informazione *on-line*. Il tema delle contro-narrazioni, nell'ottica del superamento del pubblico/privato, è affrontato da G. LOVINK, tra i cui scritti si rinvia in particolare a *Ossessioni collettive: critica dei social media*, trad. it., Milano, 2012.

modo, non può che sperarsi che i criteri per la rimozione siano concordati dai maggiori operatori del settore di concerto con le Autorità Garanti: solo per questa via è, infatti, possibile scongiurare soluzioni nazionali o arbitri da parte di soggetti (i gestori dei motori di ricerca) che non possono essere investiti di poteri pubblicistici.

5. Danno da permanenza nei risultati della ricerca?

Lo scenario immaginato si presenta a tinte ancora più fosche nel momento in cui si passa dall'analisi del diritto comunitario a quello del diritto nazionale.

In sede di recepimento della direttiva sulla tutela dei dati personali, il legislatore italiano ha fatto ricorso all'art. 2050 c.c. per valutare la responsabilità del soggetto che cagiona danni ad altri per effetto del trattamento di dati personali (art. 18, l. 31 dicembre 1996, n. 675⁵² poi 'riprodotto' nell'art. 15 del D. Lgs. 196/2003⁵³).

⁵² In argomento, v. S. SICA, *Commento* ub art. 18, in E. GIANNANTONIO - M. G. LOSANO - V. ZENO-ZENCOVICH, *La tutela dei dati personali. Commentario alla l. 675/96*, Padova, 1997, 176 ss.; M. FRANZONI, *Dati personali e responsabilità civile*, in *Resp. civ. prev.*, 1998, pp. 902 ss.; G. COMANDÈ, *Danni cagionati per effetto del trattamento dei dati personali*, in F.D. BUSNELLI - C.M. BIANCA, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 482 ss.; F.D. BUSNELLI, *Il «trattamento dei dati personali» nella vicenda dei diritti della persona: la tutela risarcitoria*, in V. CUFFARO - V. RICCIUTO - V. ZENO-ZENCOVICH, *Trattamento dei dati e tutela della persona*, Milano, 1998, 177 ss.; G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, *Dir. inf.*, 1997, pp. 703 ss.; D. CARUSI, *La responsabilità*, in V. CUFFARO - V. RICCIUTO, *Il trattamento dei dati personali*, 2ª ed., Torino, 1999, pp. 356 ss.; R. CLARIZIA, *Legge 675/96 e responsabilità civile*, in *Dir. inf.*, 1998, pp. 35 ss.; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, pp. 350 ss.; M. BIN, *Privacy e trattamento dei dati personali*, in *Contr. e impr./Europa*, 1997, p. 459 s.; E. GIANNANTONIO, *Responsabilità civile e trattamento dei dati personali*, in *Dir. inf.*, 1999, pp. 1035 ss.; C. PULIGHEDDU, *Trattamento dei dati personali e responsabilità da esercizio di attività pericolose*, in *Resp. com. impr.*, 1998, 445 ss.; V. ROPPO, *La responsabilità civile per trattamento di dati personali*, in *Danno e resp.*, 1997, 660 ss.

⁵³ Sull'art. 15 del Codice privacy si rinvia, tra gli altri, a S. SICA, *'Danno' e 'nocumento' nell'illecito trattamento di dati personali*, in *Dir. Inf.*, 2004, pp. 715 ss.; W. SARESELLA, *Danni cagionati per effetto del trattamento*, in AA.VV., *Codice della privacy*, Milano, 2013; F. GRITTI, *La responsabilità civile nel trattamento dei dati personali*, in AA.VV., *Il Codice del trattamento dei dati personali*, a cura di V. Cuffaro - R. D'Orazio - V. Ricciuto, Torino, 2005; S. SICA, *Le tutele civili*, in Aa.Vv., *Il codice dei dati personali. Temi e problemi*, a cura di F. Cardarelli - S. Sica - V. Zeno-Zencovich, Milano, 2004, pp. 541 ss.; A. MAIETTA, *Commento all'art. 15*, in *La nuova disciplina della privacy*, a cura di S. Sica - P.

L'assimilazione del trattamento dei dati personali ad un'attività pericolosa risponde all'esigenza, invero affermata già dall'art. 23 della direttiva 95/46/CE, di agevolare il ristoro degli eventuali danni subiti dai soggetti interessati per illecito trattamento dei dati personali. L'applicazione di un criterio di imputazione di natura speciale⁵⁴, a carattere oggettivo⁵⁵ (o, secondo altri, semiogettivo⁵⁶ o intermedio⁵⁷), determina, da un lato, la semplificazione della posizione del danneggiato, che sarà tenuto a provare solo il danno e il nesso eziologico, e, dall'altro lato, l'aggravamento della posizione del titolare del trattamento, che, al contrario, dovrà dimostrare di aver adottato tutte le misure necessarie ad evitare il verificarsi del danno.

Occorre però sgombrare il campo da un possibile equivoco. Ammettiamo che la Corte di Giustizia abbia effettivamente ribadito l'esistenza di un diritto alla cancellazione del dato (riconosciuto, a livello nazionale, dall'art. 7 del Codice *privacy*), quale declinazione del diritto all'oblio⁵⁸. Non è, tuttavia, sufficiente la mancata rimozione del risultato della ricerca per aversi risarcimento: il soggetto interessato, infatti, dovrà in ogni caso dimostrare di aver subito un danno dalla permanenza del collegamento ipertestuale⁵⁹.

Stanzione, Torino, 2004, pp. 66 ss.

⁵⁴ Sulla nozione di responsabilità speciali cfr. AA.VV., *Le responsabilità speciali. Modelli italiani e stranieri*, a cura di G. Autorino Stanzione, Napoli, 1994, *passim*.

⁵⁵ Per tutti, P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, pp. 54 ss.

⁵⁶ Così F.D. BUSNELLI, *La parabola della responsabilità civile*, in *Riv. crit. dir. priv.*, 1988, p. 643.

⁵⁷ Cfr. *Relazione al Codice civile*, n. 795: «Sulla materia non si è creduto di adottare alcuna delle soluzioni estreme: né quella che annetterebbe a tali attività una responsabilità oggettiva, né quella che vi ricollegherebbe l'ordinaria responsabilità per colpa. Si è adottata invece una soluzione - intermedia per la quale, sempre mantenendo la colpa a base della responsabilità, non solo si è posta a carico del danneggiante la prova liberatoria, ma si è ampliato il contenuto del dovere di diligenza, che è posto a suo carico». In questo senso, in dottrina, sebbene con alcune incertezze, V. GERI, *Le attività pericolose e la responsabilità*, in *Dir. prat. assic.*, 1961, 302; G. GENTILE, *Responsabilità per l'esercizio di attività pericolose*, in *Resp. civ. prev.*, 1950, pp. 100 ss.

⁵⁸ Sostengono che il diritto all'oblio, così come strutturato nella proposta di direttiva, sia in realtà un diritto alla cancellazione, sia F. PIZZETTI, *Il prisma del diritto all'oblio*, in AA.VV., *Il caso del diritto all'oblio*, cit., p. 62; che A. MANTELEO, *Il diritto all'oblio dalla carta stampata ad Internet*, cit., pp. 166-167.

⁵⁹ Ancora A. PALMIERI - R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, cit., 6, i quali osservano che non sarebbe «comunque configurabile l'obbligo di accogliere le istanze di eliminare dall'indice dati personali, lecitamente pubblicati nel cyberspazio, soltanto perché sgraditi all'interessato che-non potendo ottenerne la cancellazione o la modifica- desidera confinarli in un anatro arduo da raggiungere per l'ordinario internauta».

Un esempio può chiarire il punto. Ipotizziamo che un utente chieda la rimozione di un risultato della ricerca e che l'operatore, per incuria o perché ritiene che la richiesta sia infondata, non si attivi. A questo punto, l'utente potrà rivolgersi, in via alternativa, al Garante o all'Autorità giudiziaria: nel primo caso, per ottenere un ordine di cancellazione; nel secondo caso, come già verificatosi nella giurisprudenza francese⁶⁰, tale ordine potrà essere eventualmente accompagnato da una penale per il ritardo⁶¹.

Per accedere ad una tutela risarcitoria, però, l'utente dovrà provare di aver subito un pregiudizio dalla permanenza del collegamento ipertestuale: si pensi, completando l'esempio menzionato, al caso in cui il soggetto invii un proprio curriculum vitae e sia scartato dalla selezione a causa della notizia del suo coinvolgimento, molti anni prima, in una vicenda giudiziaria⁶².

⁶⁰ Cfr. TGI Parigi, ord., 15 febbraio 2012, cit.

⁶¹ Rimarca la necessità di un *enforcement* per il diritto all'oblio M. SIANO, *Il diritto all'oblio in Europa e il recente caso spagnolo*, in AA.VV., *Il caso del diritto all'oblio*, cit., p. 131.

⁶² Cfr. Garante per la protezione dei dati personali, 7 luglio 2005. Nel caso di specie, l'Autorità ha ritenuto eccedente il principio di essenzialità dell'informazione, di cui al Codice deontologico dei giornalisti, la diffusione di un video di un processo svoltosi sedici anni prima, che riprendeva una persona presente in aula nel pubblico, ma estranea al processo e coinvolta esclusivamente in virtù di un legame sentimentale con uno degli imputati. Nel provvedimento in questione, l'Autorità ha confermato che tale diffusione sarebbe illecita, considerato il diritto «della segnalante di non essere più ricordata pubblicamente, anche a distanza di molti anni» per una «delicata vicenda giudiziaria e personale, già a suo tempo oggetto di un'ampia attenzione da parte del pubblico e dei mezzi di informazione». Il filmato, quindi, non avrebbe rispettato «la propria rinnovata dimensione sociale e affettiva così come si è venuta definendo successivamente alla vicenda stessa, anche in relazione al proprio diritto all'identità personale e al diritto alla protezione dei dati personali». L'obiettivo del diritto all'oblio deve essere infatti quello di «ricostruire la dimensione sociale dell'individuo, evitando che la vita passata possa costituire un ostacolo per la vita presente»: così testualmente M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009, p. 121. In termini simili si esprimono sia M.R. MORELLI, *Oblio (diritto all')*, in *Enc. dir.*, agg. VI, Milano, 2002, p. 848, che C. CHIOLA, *Appunti sul c.d. diritto all'oblio e tutela dei dati personali*, in *Percorsi cost.*, 2010, I, p. 38; G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. Inf.* 2010, p. 395. Nella giurisprudenza italiana, v. Trib. Milano, 26/04/2013, <http://www.openmediacoalition.it/documenti/trib-milano-sez-i-sent-26-04-2013/> [consultato il 30/09/2014] secondo cui il diritto all'oblio «salvaguarda la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita (stante il lasso di tempo intercorso dall'accadimento del fatto che costituisce l'oggetto) di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità». Interessante, sul punto, il caso Mosley, nel quale è stata chiesta la deindicizzazione dopo che l'High Court of Justice aveva stabilito

Non sussiste, quindi, un automatismo – che, anzi, va scongiurato – tra mancata cancellazione e risarcimento, dovendosi ritenere, sulla scorta delle regole generali che governano l'illecito aquiliano, che il danno non possa essere *in re ipsa*.

6. Conclusioni

In conclusione, è forte l'impressione che il rimedio ordinato dalla Corte di Giustizia sia peggiore del male. Non si vuole in alcun modo negare cittadinanza al diritto all'oblio⁶³; semplicemente, si vuole avvertire che, percorrendo i sentieri tracciati dalla sentenza dello scorso maggio, ci si incammina verso un percorso tortuoso, che rischia di riesumare gli spettri ingabbiati dalla direttiva sul commercio elettronico. Ci si riferisce alla possibilità che gli intermediari della rete divengano arbitri delle informazioni accessibili, operando una selezione non solo della quantità delle informazioni, ma altresì della loro qualità. Eliminando, senza eccessivi scrupoli e perché incentivati e legittimati a farlo, i contenuti scomodi ed invisibili a taluno⁶⁴.

Non stiamo evocando, pare opportuno precisarlo, il pericolo di conseguenze censorie⁶⁵, né, d'altro canto, stiamo negando il potere economico e

l'illiceità della diffusione delle immagini, cfr. *Mosley v News Group Newspapers* [2008] EWHC 1777 (QB).

⁶³ Da ritenersi, come osserva T.E. FROSINI, *Il diritto all'oblio e la libertà informatica*, in AA.VV., *Il caso del diritto all'oblio*, cit., 94, quale corollario della dignità dell'uomo riconosciuta dall'ordinamento tedesco e poi dalla Carta dei diritti fondamentali. Sul concetto di dignità, v. G. RESTA, *Dignità*, in *Tratt. di biodiritto*, diretto da S. Rodotà - P. Zatti, vol. I, *Ambito e fonti del biodiritto*, Milano, 2010, pp. 259 ss.

⁶⁴ Il richiamo è a S. RODOTÀ, *Libertà, opportunità, democrazia e informazione*, in *Internet e privacy: quali regole?*, Atti del Convegno di Roma, 8-9 maggio 1998, Cittadini e Società dell'informazione, Supplemento n. 1 al Bollettino n. 5 del Garante, 1998, 15, che, a proposito degli ISP, paventò il rischio che potessero divenire dei «censori istituzionali». Sostiene che la possibilità di intervento non sia conforme «all'attività di un motore di ricerca che è solo diffusore, e non editore (*editor*)», delle notizie rese disponibili attraverso l'interrogazione del database del motore e il recupero dei dati dai vari siti *web*» F. PIZZETTI, *Il prisma del diritto all'oblio*, in AA.VV., *Il caso del diritto all'oblio*, cit., p. 48. Il rischio che la sentenza in esame possa avere dei riflessi sull'operato degli ISP è evidenziato da O. POLLICINO, *Google rischia di «vestire» un ruolo para-costituzionale*, in *Il Sole-24 Ore* del 15 maggio 2014.

⁶⁵ Più catastrofista, invece, J. ROSEN, *The Right to be Forgotten*, 64 *Stan. L. Rev. Online* 88, 92: «This could transform Google, for example, into a censor-in-chief for the

politico oramai rivestito dai grandi operatori del web, i cc.dd. *over-the-top*, nella consapevolezza che la bipartizione tra apocalittici e integrati, nelle discussioni che hanno investito i dilemmi sollevati dall'avvento di internet negli ultimi due decenni, non ha fatto altro che aggravare i problemi, anche nei casi in cui le soluzioni erano agevolmente perseguibili⁶⁶.

Tuttavia, a nostro modesto avviso, questioni come quelle in oggetto, che investono interessi costituzionalmente garantiti, ma talora contrapposti, non possono essere risolte né a livello giudiziario, né a livello nazionale – come parte della dottrina statunitense, che propugna un'applicazione universale di precetti 'sacri', ma locali, come quelli sanciti nel *First Amendment* –, né, ancora, a livello comunitario, giacché, e ci sia consentita la metafora sportiva, le fughe in avanti impongono, ad un certo punto del tragitto, di attendere il gruppo. In altri termini, la polarizzazione a cui si sta assistendo sulle due sponde dell'Oceano⁶⁷ in merito alla tutela del diritto all'oblio rende complesso il dialogo e dimostra che né il *laissez-faire* e le logiche del *free market* americane⁶⁸, né la tentazione pan-europeista dell'art. 17 della

European Union, rather than a neutral platform».

⁶⁶ Si pensi, ad esempio, al caso del *copyright*, in cui si è assistito per anni ad uno scontro tra titolari dei diritti e ISP, senza ipotizzare soluzioni, come quella sostenuta oggi da C.MANARA, *Attacking the Money Supply to Fight Against Online Illegal Content?*, Edhec Business School Research Centre, 2012, che miravano ad attaccare i flussi monetari e non quelli di informazione. Non è un caso che l'approccio indicato come *follow the money* sia successivamente stato ripreso – seppur solo sul piano meramente declamatorio – dal Regolamento AGCom sulla tutela del diritto d'autore; per una critica a tale richiamo meramente verbale, privo di riscontri applicativi, sia consentito rinviare a G.M. RICCIO, *The New Italian Regulation on Copyright Enforcement: Comparative and Critical Remarks*, 5 *J. of Intell. Prop. Information Tech. and E-Commerce Law* (2014) in corso di pubblicazione.

⁶⁷ Peraltro, dall'analisi delle singole esperienze europee, non sembra possibile – prima dell'approvazione del Regolamento comunitario – sostenere l'esistenza di un modello unico europeo: cfr., sul punto, l'interessante rassegna di O. POLLICINO - M. BASSINI, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, in AA.VV., *Il caso del diritto all'oblio*, cit., pp. 190 ss.

⁶⁸ Ritieni che, insieme al *free speech*, sia questo lo scoglio che rende riluttante l'ordinamento statunitense a riconoscere pienamente un diritto alla tutela dei dati personali, così come avvenuto in Europa, J.Q. WHITMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 *Yale L.J.* pp. 1151, 1208 (2004). Nello stesso senso, v. anche J. ROSEN, *The Right to be Forgotten*, 64 *Stan. L. Rev. Online* 88 (2012). Secondo R.K. WALKER, *The Right to Be Forgotten*, 64 *Hastings L.J.* p. 257 (2012), il principale problema alla determinazione di un unico diritto all'oblio sarebbe dato dal fatto che, negli USA, la *privacy* sarebbe intesa come tutela dall'interferenza del potere; in Europa, invece, come forma di tutela della propria reputazione. Sostiene, invece, che il *right to be forgotten*, negli Stati Uniti, non supererebbe lo scrutinio della Corte Suprema F. WERRO, *The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash*, in *Liability in the Third Millennium*,

proposta di Regolamento possono essere una risposta appagante a problematiche che richiedono, inevitabilmente, soluzioni condivise⁶⁹.

Abstract

The decision of the European Court of Justice on the right to be forgotten should dramatically change the internet environment. Google, as well as all the other search engine operators, has implemented a search removal request aimed at facilitating users' requests of cancellation of personal data. However the ECJ has not specified what are the criteria to be followed by search engine operators in order to comply with the data protection regulation. Is this uncertainty jeopardizing the neutrality principle of the e-commerce directive? Starting from the provision held by the DMCA and the e-commerce directive on ISPs liability, the article offers a comprehensive overview of notice and take-down procedures for copyright infringements, discussing how such procedures could influence the search removal request implemented by the main search engines and its criteria

A. Colombi Ciacchi, C. Godt, P. Rott, L.J. Smith (eds.), Baden-Baden, F.R.G., 2009, p. 294.

⁶⁹ In merito alle proposte statunitensi di disciplinare il *right to be forgotten* si rinvia a M.L. AMBROSE - J. AUSLOOS, *The Right to be Forgotten Across the Pond*, 3 *J. of Information Policy* p. 8 (2013).

Roberto Flor

Dalla 'Data retention' al diritto all'oblio. dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive 'de jure condendo'

SOMMARIO: 1. Premessa - 2. I fatti all'origine della decisione Google/Spagna - 3. Le principali linee argomentative della Corte - 4. Tutela della riservatezza *versus* interesse all'accertamento e alla prevenzione dei reati. Uno sguardo ai più recenti sviluppi in Europa - 5. La sentenza della Corte di Giustizia sulla c.d. *data retention*: un importante passo per il rafforzamento del diritto alla riservatezza. Ma con quali effetti per il sistema di giustizia penale? - 6. Verso una definizione del 'diritto all'oblio' - 6.1. Il diritto all'oblio nelle conclusioni dell'Avvocato Generale - 6.2. Il diritto all'oblio nella proposta di regolamento europeo concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) - 7. Verso una definizione 'integrata' del diritto all'oblio e possibili linee guida per il bilanciamento con le esigenze proprie del sistema di giustizia penale: fra proposte *de jure condendo* e prospettive *de jure condito* - 8. Conclusioni

1. Premessa

«Chi controlla il passato, controlla il futuro; chi controlla il presente, controlla il passato [...] Credi davvero che il passato abbia un'esistenza reale? [...] Il passato esiste forse concretamente nello spazio? C'è da qualche parte un luogo, un mondo di oggetti solidi, dove il passato sta ancora avvenendo? [...] Dove esiste il passato, seppure esiste?»

«Nei documenti. È registrato lì il passato [...] Nei documenti. E...nella mente. Nella memoria degli uomini»¹.

Questo passo rappresenta forse una delle massime espressioni della paura orwelliana della perdita di memoria storica indotta dai mezzi di informazione, seppur legata al totalitarismo, alla corruzione del linguaggio

¹ Tratto da G. ORWELL, 1984, I ed. originale, 1949.

ed alla perdita dell'identità individuale. Esso risulta però attuale, in particolare nell'odierna società di Internet, in cui la 'memoria' o il 'passato' vivono nella rete e possono contribuire alla ricostruzione di avvenimenti, al riconoscimento di persone scomparse o di pregiudicati, nonché all'individuazione di vittime della pedopornografia *online*, solo per riportare alcuni casi, anche tramite video o registrazioni caricate dagli utenti in siti *user generated content* e indicizzati dai motori di ricerca.

La sentenza del 13 maggio 2014 della Corte di Giustizia sul c.d. caso Google/Spagna è immediatamente passata alle cronache come la decisione che ha riconosciuto il c.d. 'diritto all'oblio'². In verità la controversia, sul piano sociale prima ancora che su quello del diritto penale sostanziale, è rilevante per tutto il sistema di giustizia penale, risulta essere più complessa, in quanto coinvolge questioni attinenti non solo ai possibili profili di responsabilità del fornitore di un servizio nella società dell'informazione e di Internet, ai limiti degli 'ordini' delle 'autorità competenti' di rimozione di dati e informazioni per la tutela della riservatezza in rapporto al bilanciamento con gli altri diritti fondamentali coinvolti ed il perseguimento di interessi di rilevanza collettiva, ma anche ai profili distopici che talvolta si vogliono attribuire a Internet, quale '*wild west*' della globalizzazione del crimine³, portato a estremi apocalittici.

Non è certo la prima volta che la Corte di Giustizia ha dovuto affrontare problematiche riguardanti proprio il bilanciamento fra le diverse esigenze, da un lato, di tutela dei diritti fondamentali e, dall'altro, di accertamento e prevenzione di attività illecite e di reati.

In alcuni precedenti recenti⁴ la Corte ha valorizzato, in particolare, i diritti tutelati dagli artt. 8 e 11 della Carta dei diritti fondamentali dell'Unione europea (Carta), oltre alla libertà di impresa (*ex art. 16 della Carta*)

² Corte di Giustizia dell'Unione europea, sent. 13 maggio 2014 (C-131/12). Per i primi commenti si rinvia a B. VAN ALSENOY, A. KUCZERAWY AND J. AUSLOOS, *Search engines fter Google Spain: internet@liberty or privacy@peril?*, in *ICRI*, 15/2013, pp. 1-74; G. FINOCCHIARO, *Editoriale*, in *Giustizia civile. com.*, 2014, 3 e ss.; A. PALMIERI, R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi Quaderni del Foro Italiano*, 1, 2014, pp. 1-16.

³ Vedi B. SANDYWELL, *On the globalization of crime: the Internet and new criminality*, in Y. JEWKES, M. YAR, *Handbook of Internet Crime*, Willan Publishing, 2010, pp. 38 e ss. Cfr., inoltre, R. FLOR, *Social Networks e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Riv. trim. dir. pen. ec.*, 2012, pp. 647-694, anche per gli ulteriori riferimenti bibliografici.

⁴ Corte di Giustizia dell'Unione europea, sent. 24 novembre 2011 (C-70/10) e 16 febbraio 2012 (C-360/10), nonché, in termini parzialmente diversi, Corte di Giustizia dell'Unione europea, sent. 27 marzo 2014 (C-314/12). Vedi *infra*, nota 5.

per garantire la loro prevalenza nel bilanciamento con le esigenze di tutela della proprietà intellettuale in Internet, le cui violazioni costituiscono, in molti Stati, un illecito penale⁵. Pur trattandosi di questioni pregiudiziali

⁵ Cercando di sintetizzare, in due casi (C-70/10 e C-360/10) la Corte ha affermato che l'ingiunzione diretta, da parte di un giudice nazionale ad un *service provider*, di adottare sistemi di filtro per impedire agli utenti di utilizzare sistemi di *file sharing* in violazione delle norme in materia di diritto d'autore, comprime in modo sproporzionato tali diritti. Le ragioni di queste decisioni si fondano sul fatto che un sistema di filtro adottato da un fornitore di servizi presuppone l'identificazione degli utenti e, nell'ambito delle comunicazioni elettroniche, i *file* che appartengono al traffico *peer-to-peer* e i *file* che contengono opere sulle quali i titolari dei diritti di proprietà intellettuale affermino di vantare diritti. Tale sistema è in grado di determinare, dunque, quali tra questi *file* siano scambiati in modo illecito, procedendo al blocco delle relative condivisioni. Questo tipo di sorveglianza attiva e preventiva, senza limiti di tempo e a totale carico, sul piano economico, del prestatore di servizi, richiederebbe un'osservazione attiva sulla totalità delle comunicazioni elettroniche e, indistintamente, degli utenti che si avvalgono del servizio. In questi casi, dunque, la Corte ha bene evidenziato che non può desumersi che la tutela del diritto di proprietà intellettuale, sebbene sia sancita dall'art. 17, par. 2, della Carta, sia intangibile e assoluta, rispetto alla tutela di altri diritti fondamentali, come quelli previsti dagli artt. 8, 11 e 16 della Carta. Si consenta di rinviare a R. FLOR, *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet*, Padova, 2010 che, con riferimento a fenomeni criminali che trovano in Internet un mezzo formidabile per la loro commissione, oppure l'ambiente ideale di manifestazione, riporta la disciplina penale di alcuni paesi (in particolare Italia, Germania, Francia, Spagna, Regno Unito, Svezia e Stati Uniti d'America). Con riferimento alle cause C-70/10 e C-360/10 vedi l'art. 87, n. 1, primo e secondo comma, della legge belga 30 giugno 1994 (*Belgisch Staatsblad*, 27 luglio 1994), sul diritto d'autore e sui diritti connessi, il quale prevede quanto segue: «Il presidente del *Tribunal de première instance* (...) consta[ta] l'esistenza e [ordina] la cessazione di qualsiasi violazione del diritto d'autore o di un diritto connesso. [Può] altresì emanare un provvedimento inibitorio contro intermediari i cui servizi siano utilizzati da un terzo per violare il diritto d'autore o un diritto connesso». Cfr. R. FLOR, *Lotta alla «criminalità informatica» e tutela di «tradizionali» e «nuovi» diritti fondamentali nell'era di Internet*, in *Dir. pen. cont.*, 20 settembre 2012, pp. 11 e ss. In una più recente pronuncia, invece, la Corte ha ritenuto che i diritti fondamentali riconosciuti dal diritto dell'Unione devono essere interpretati nel senso che non ostano a che sia vietato, con un'ingiunzione pronunciata da un giudice ad un fornitore di accesso ad Internet, di concedere ai suoi abbonati l'accesso ad un sito Internet che metta in rete materiali protetti senza il consenso dei titolari dei diritti, qualora tale ingiunzione non specifichi quali misure il fornitore d'accesso deve adottare e quest'ultimo possa evitare sanzioni per la violazione di tale ingiunzione dimostrando di avere adottato tutte le misure ragionevoli. A condizione, tuttavia, che da un lato, le misure adottate non privino inutilmente gli utenti di Internet della possibilità di accedere in modo lecito alle informazioni disponibili e, dall'altro, che tali misure abbiano l'effetto di impedire o, almeno, di rendere difficilmente realizzabili le consultazioni non autorizzate dei materiali protetti e di scoraggiare seriamente gli utenti di Internet che ricorrono ai servizi del destinatario di questa stessa ingiunzione dal consultare tali materiali messi a loro disposizione in violazione del diritto di proprietà

sull'interpretazione delle direttive 2000/31/CE sul commercio elettronico, 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, 2004/48/CE sul rispetto dei diritti di proprietà intellettuale, 95/46/CE sul trattamento dei dati personali e 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, esse hanno, di fatto, posto in discussione l'uso di taluni mezzi tecnologici 'invasivi' rispetto alla tutela dei diritti fondamentali, ferma restando la validità degli atti europei. Con la sentenza del 13 maggio 2014 (c.d. caso Google/Spagna), invece, la Corte di Giustizia ha affermato la prevalenza dei diritti tutelati dagli artt. 7 e 8 della Carta, in determinate condizioni, rispetto alla libertà di espressione e agli interessi economici dei *providers*, rafforzando in questo modo la posizione giuridica della persona interessata da un trattamento di dati personali, benché non sia pacifico poter ricavare dalle norme della direttiva 95/46, interpretate alla luce delle disposizioni dalla Carta, un diritto 'generalizzato' all'oblio⁶.

Questa sentenza giunge dopo un'altra importante decisione (c.d. caso *data retention*)⁷, in cui i Giudici di Lussemburgo hanno affrontato per la prima volta la delicata questione concernente il bilanciamento fra le esigenze di repressione ed accertamento dei reati e la tutela dei diritti fondamentali dell'individuo, che possono essere fortemente limitati dagli obblighi di conservazione dei dati di traffico telefonico e telematico nella società informazione, annullando la direttiva 2006/24 perché contraria agli artt. 7, 8 e 11 della Carta dei diritti fondamentali dell'Unione europea. In quest'ultima sentenza la Corte ha esaminato gli obblighi di conservazione dei dati nell'UE alla luce dei principi di necessità e proporzionalità, tenuto conto e nell'interesse della sicurezza nazionale, del buon funzionamento del mercato interno e del rafforzamento del rispetto della vita privata, nonché del diritto fondamentale alla protezione dei dati personali, fornendo alcune linee guida essenziali, che si inseriscono inevi-

intellettuale, circostanza che spetta alle autorità e ai giudici nazionali verificare. Vedi Corte di Giustizia dell'Unione europea, 27 marzo 2014 (C-314/12).

⁶ Vedi, in questo senso, le conclusioni dell'Avvocato Generale Niilo Jääskinen presentate il 25 giugno 2013.

⁷ Vedi Corte di Giustizia dell'Unione europea, sent. 8 aprile 2014 (C-293/12 e C-594/12), con primo commento di R. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in http://www.penalecontemporaneo.it/upload/1398628841F_LOR_2014.pdf [consultato il 30/09/2014], a cui si rinvia per gli ulteriori riferimenti bibliografici. Cfr. anche E. COLOMBO, *Data retention e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della Direttiva 2006/24/CE*, in *Cass. pen.*, 7/8, 2014, pp. 2705 e ss.

tabilmente nel contesto più ampio della riforma in atto, a livello europeo, di tutta la disciplina in materia di tutela della *privacy*, attraverso un *corpus* unico di norme⁸. Queste ultime due decisioni, in particolare, se da un lato rafforzano la tutela della riservatezza, dall'altro segnano uno strappo epocale nell'odierna società di Internet, ponendo dei limiti decisi all'uso delle tecnologie e della rete, che non sempre possono produrre effetti positivi rispetto alla tutela di rilevanti interessi di natura generale e collettiva.

2. I fatti all'origine della decisione Google/Spagna

Il 5 marzo 2010, il sig. Costeja González, cittadino spagnolo, ha presentato dinanzi all'*Agencia Española de Protección de Datos* (AEPD) un reclamo contro il quotidiano *La Vanguardia Ediciones SL* e contro Google Spain e Google Inc., in quanto gli utenti di Internet, introducendo il suo nome in «Google Search», ottenevano dei *link* verso due pagine del quotidiano pubblicate nel 1998, sulle quali figurava un annuncio di rilevanza giudiziaria. Egli chiedeva, quindi, che fosse ordinato alla testata giornalistica di sopprimere o modificare tali pagine, oppure di ricorrere a taluni strumenti forniti dai motori di ricerca per proteggere i dati, ordinando altresì a Google Spain o a Google Inc. di eliminare o di occultare le informazioni personali, in modo che cessassero di comparire tra i risultati di ricerca.

Il reclamo è stato accolto parzialmente. L'AEPD, infatti, ha ordinato ai soli gestori del motore di ricerca di rimuovere i dati e di provvedere ad impedire l'accesso alle informazioni.

ssa ha ritenuto, da un lato, che la grave ingerenza nei diritti fondamentali tutelati dagli artt. 7 e 8 della Carta non possa essere giustificata dal semplice interesse economico del fornitore del servizio. Dall'altro lato, però, poiché la soppressione di *link* dall'elenco dei risultati potrebbe, a seconda della natura e del tipo di informazione, avere ripercussioni sul legittimo interesse degli utenti ad avere accesso a quest'ultima, occorrerebbe ricercare comunque, caso per caso, un 'giusto equilibrio' fra i diritti fondamentali coinvolti.

Contro tale decisione Google Spain e Google Inc. hanno proposto

⁸ Si fa riferimento alle concrete iniziative europee. In questa sede basti il rinvio a: http://ec.europa.eu/justice/data-protection/index_en.htm [consultato il 30/09/2014].

ricorso davanti all'*Audiencia Nacional*, la quale ha sospeso il procedimento ed ha sottoposto alla Corte di Giustizia alcune questioni pregiudiziali riguardanti, in particolare, i limiti degli obblighi che possono incombere in capo ai gestori di motori di ricerca per la tutela dei dati personali delle persone che non desiderino che alcune informazioni a loro collegate, pubblicate sui siti *web*, vengano localizzate, indicizzate e/o messe a disposizione degli utenti in Internet.

Più precisamente i quesiti posti alla Corte possono essere ricondotti in 4 gruppi, riguardanti: 1. l'ambito territoriale di applicazione della direttiva; 2. l'attività dei motori di ricerca quali fornitori di contenuti ossia, *in primis*, se essa possa essere riconducibile alla nozione di 'trattamento di dati' *ex art. 2, lett. b)* della direttiva e, in secondo luogo, se la società di gestione di tali motori possa ritenersi un 'responsabile del trattamento' ('titolare') *ex art. 2, lett. d)* della medesima direttiva; 3. i 'poteri' dell'A-EPD, ossia se possa ordinare al *provider* di rimuovere le informazioni pubblicate da terzi, e rimanenti nella *web* page di origine, a prescindere sia dalla natura (lecita o illecita) della pubblicazione, sia dall'autorizzazione del titolare della pagina *web* in cui essa è inserita; 4. la portata del diritto di cancellazione e di opposizione al trattamento dei dati in rapporto al c.d. diritto all'oblio e alla libertà di espressione.

Sul piano strettamente penalistico, in questa sede, non saranno approfondite le questioni attinenti all'ambito territoriale ed alle nozioni di 'trattamento' e di 'responsabile del trattamento' (titolare), se non tramite brevi richiami alle precise argomentazioni della Corte, ma sarà dedicata più specifica attenzione ai quesiti di cui ai punti 3 e 4, che coinvolgono anche le problematiche attinenti ai limiti degli 'ordini' delle 'autorità competenti' di rimozione di dati e informazioni per la tutela della riservatezza in rapporto al bilanciamento con gli altri diritti fondamentali coinvolti e l'interesse al perseguimento dei reati. La sussistenza di un obbligo a carico del gestore di un motore di ricerca, che può comportare la rimozione di informazioni personali, deve essere affrontata tenendo presente le disposizioni della direttiva 2000/31 (c.d. direttiva *e-commerce*) ed il dibattito inerente alla natura di *provider* di Google. In questa sede non potranno essere approfondite anche queste tematiche⁹. Le disposizioni della direttiva

⁹ Basti il rinvio, in questa sede, e con specifico riferimento ai profili penalistici, a L. PICOTTI, *Fondamento e limiti della responsabilità penale dei Service Providers in Internet*, in *Dir. pen. proc.*, 1999, pp. 379 ss.; L. PICOTTI, *La responsabilità penale dei Service Providers in Italia*, in *Dir. pen. proc.*, 1999, pp. 501 ss.; D. DE NATALE, *La responsabilità dei fornitori di informazioni in Internet per i casi di diffamazione on line*, in *Riv. trim. dir. pen. ec.*, 2009, pp. 509 ss.; R. FLOR, *Social networks e violazioni penali*, cit.; cfr. anche D. PETRINI,

e-commerce, comunque, verranno considerate in quanto, da un lato, i possibili obblighi derivanti dalla direttiva 95/46 devono essere tenuti distinti dagli obblighi derivanti dall'applicazione della direttiva *e-commerce*; dall'altro lato, però, i fatti oggetto della richiesta di rimozione o cancellazione possono avere rilevanza penale, ovvero costituire dati e informazioni utili per un'indagine penale. Inoltre, mentre l'esercizio del diritto all'oblio potrebbe coinvolgere dati e trattamenti di dati non necessariamente illeciti o a contenuto illecito, i 'procedimenti' e i 'meccanismi' ingiunzionali previsti dalla direttiva *e-commerce* riguardano l'esercizio di 'attività illecite' o 'illegalì', anche se non sempre di rilevanza penale.

3. Le principali linee argomentative della Corte

In estrema sintesi, nel c.d. caso Google/Spagna la Corte ha affermato che l'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione

La responsabilità penale per i reati via Internet, Napoli, 2004. Più di recente, e con riferimento al noto caso Google/Vividown, A. INGRASSIA, *Il ruolo dell'isp nel cyberspazio: cittadino, controllore o tutore dell'ordine? Risposte attuali e scenari futuribili di una responsabilità penale dei provider nell'ordinamento italiano*, in L. LUPÁRIA (cur.), *Internet provider e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, Milano, 2012, pp. 47 e ss. Sul citato caso vedi da ultimo Cass. pen., sez. III, 17 dicembre 2013 (dep. 3 febbraio 2014), n. 5107. Preme evidenziare che gli obblighi di rimozione degli effetti derivanti da 'fatti' già realizzati (così anche gli artt. 14, co., 3, 15, co. 2 e 16, co. 3, d.lgs. n. 70/2003, che attuano fedelmente le disposizioni della direttiva *e-commerce*), e quelli di segnalazione di illeciti (art. 17, co. 2, dello stesso d.lgs. n. 70/2003) 9, nonché la medesima disposizione che vieta un obbligo generale di sorveglianza, fanno riferimento a 'violazioni' ed 'attività illecite' e non a 'reati'. Pertanto esse presuppongono certamente (ad esclusione dell'ultima norma citata) 'attività', come detto, già verificatesi. Ma tali attività non necessariamente costituiscono già un reato o un 'fatto' di rilevanza penale. Essi individuano, dunque, 'situazioni di rischio', se non violazioni, che possono anche avere rilevanza penale, ma che non necessariamente, però, costituiscono già un reato perfezionato. Si tratta comunque di attività che si svolgono sotto l'autorità o il controllo del *provider*, rispetto alle quali è dotato di un effettivo potere / dovere di interferenza — in quanto viene a conoscenza dell'illecito o è messo concretamente in grado di riconoscerlo, ossia in condizione di riconoscere la situazione di pericolo o di rischio — per impedire sia la prosecuzione delle violazioni che la realizzazione di reati, se le condizioni di rischio sono specificatamente individuate e definite dai provvedimenti ingiunzionali. Pertanto non è pacifica l'esclusione di una posizione di garanzia o di un obbligo di impedimento dei reati realizzati dagli utenti della rete in capo al *provider*, la cui sussistenza deve essere valutata caso per caso anche rispetto agli obblighi previsti dalla disciplina extrapenale del 'settore di riferimento' (pedopornografia, proprietà intellettuale, *privacy* ecc.).

dei presupposti di applicazione degli artt. 12, lett. *b*), e 14, co. 1, lett. *a*), della direttiva 95/46, possono ordinare al gestore del servizio (Google) di cancellare, dall'elenco di risultati che appare a seguito di una ricerca, i *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative a una persona. Il fornitore del servizio è obbligato, inoltre, a sopprimere gli stessi *link* anche nel caso in cui il nome o le informazioni non vengano previamente o simultaneamente cancellati dalle pagine *web* del quotidiano, eventualmente quando la loro pubblicazione sia altresì di per sé lecita. Sulla base dell'interpretazione di tali prescrizioni, dettate dall'art. 6, co. 1, lett. da *c*) a *e*), direttiva 95/46, un trattamento di dati inizialmente lecito potrebbe divenire, con il tempo, incompatibile con la direttiva, qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura, in particolare, nel caso in cui i dati risultino inadeguati, non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità e al medesimo tempo trascorso. È agevole notare che, secondo la Corte, i diritti fondamentali di cui agli artt. 7 e 8 della Carta prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico degli utenti a trovare l'informazione in occasione di una ricerca *online* relativa ad una persona determinata. Ferme restando, secondo i Giudici, le eccezioni legate, ad esempio, al ruolo ricoperto da tale persona nella vita pubblica, che potrebbe giustificare la prevalenza dell'interesse degli utenti ad avere accesso all'informazione¹⁰.

Le motivazioni della sentenza muovono, anzitutto, dalle definizioni di 'trattamento' di dati e di 'responsabile del trattamento' (o, meglio, 'titolare del trattamento'), così come previste dalla direttiva. La prima, *ex art.* 2, lett. *b*), è estremamente ampia e fa riferimento a qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione.

La Corte ha già avuto modo di affrontare la questione e ha concluso che l'operazione consistente nel far comparire su una pagina Internet dati personali deve essere considerata un «trattamento»¹¹. Nel c.d. caso *Google/Spagna* sono presenti anche informazioni riguardanti persone

¹⁰ Per quanto riguarda la situazione italiana *in subiecta materia* basti il rinvio al recente provvedimento del Garante Privacy, 10 luglio 2014, n. 353.

¹¹ Si veda caso *Lindqvist* (C-101/01, EU:C:2003:596, punto 25).

fisiche identificate o identificabili, e dunque «dati personali». Di conseguenza l'uso della rete e di un motore di ricerca comporta che il gestore di questo ultimo «raccolge», «estrae», «registra» e «organizza» tramite i suoi programmi di indicizzazione, «conserva» e, eventualmente, «comunica» e «mette a disposizione» dei propri utenti tali dati e informazioni, essendo indifferente che essi non vengano modificati dal motore di ricerca o vengano elaborati in modo automatizzato dai softwares o dagli applicativi.

Quanto alla questione se il gestore di un motore di ricerca debba essere considerato «responsabile del trattamento» dei dati personali appare decisivo il fatto che egli stesso a determina le finalità e gli strumenti della sua attività e, dunque, del trattamento di dati personali che effettua. Pertanto può essere considerato senza dubbio un «responsabile» (o, meglio, titolare *-controller*) ex art. 2, lett. *d*), della direttiva.

Il trattamento di dati personali effettuato nell'ambito dell'attività di un motore di ricerca, ad ogni modo, si distingue nettamente da quello effettuato dai gestori di siti o dagli editori di *web-sites* o testate giornalistiche *online*.

Il primo, infatti, scansiona e organizza le informazioni tramite procedimenti di indicizzazione, rinviando a pagine *web* o a contenuti presenti nella rete. Si tratta di un'attività che può essere oggetto di limitazioni da parte dei gestori dei siti, dei *social media* o dei *social networks* nonché, in alcuni casi, da parte degli utenti stessi, i quali possono richiedere di essere esclusi in tutto o in parte dagli indici automatici. Rimane però fermo un dato oggettivo, ossia che le finalità e gli strumenti anche di tale trattamento sono determinati dal gestore del motore di ricerca.

In sintesi, dunque, ex art. 2, lett. *b*) e *d*) della direttiva 95/46, da un lato, l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», se tali informazioni contengano dati personali, e, dall'altro lato, il gestore del motore di ricerca deve essere considerato «responsabile» ('titolare') del trattamento.

Ne consegue logicamente che tale trattamento di dati effettuato per le esigenze del funzionamento del motore di ricerca non è sottratto agli obblighi e alle garanzie previsti dalla direttiva per la tutela delle libertà e dei diritti fondamentali delle persone fisiche, in particolare del diritto al

rispetto della vita privata e dei dati personali (*ex* artt. 7 e 8 della Carta)¹².

Per quanto riguarda il trattamento di dati effettuato da Google, l'art. 7, lett. *f*), della direttiva 95/46, richiede di operare un bilanciamento di interessi fra i diritti coinvolti, consentendo il trattamento dei dati se risulta essere necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del terzo o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, la quale può opporsi per motivi legittimi al trattamento dei dati che la riguardano, *ex* art. 14, co. 1, lett. *a*) della direttiva.

Tale diritto può essere esercitato direttamente nei confronti del titolare del trattamento, oppure attraverso il ricorso all'autorità di controllo o all'autorità giudiziaria (artt. 12, lett. *b*), e 14, co. 1, lett. *a*) della direttiva 95/46). Considerata la potenziale gravità dell'ingerenza nell'area di 'riservatezza' pertinente alla persona, il trattamento dei dati da parte del gestore di un motore di ricerca non può essere giustificato solo sulla base di interessi di natura economica.

È vero, come affermano i Giudici, che la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest'ultima. È però altresì vero che sia la direttiva, che la Carta esigono che venga effettuato un corretto bilanciamento tra tale interesse e i diritti fondamentali della persona di cui agli artt. 7 e 8 della stessa Carta.

Il trattamento dei dati effettuato dal gestore del motore di ricerca si aggiunge a quello effettuato dagli editori di siti web, distinguendosi allo stesso tempo. Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli artt. 12, lett. *b*), e 14, co. 1, lett. *a*), della direttiva contro il gestore del motore di ricerca, ma non contro l'editore della pagina web, che potrebbe aver trattato i dati «esclusivamente a scopi giornalistici». Sulla base di queste principali argomentazioni i Giudici hanno ritenuto che nel c.d. caso

¹² Questo ultimo prevede che i dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica, e che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente. In tal senso gli Stati membri devono garantire a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento, a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non sia conforme alle disposizioni della direttiva.

Google/Spagna non sussistessero ragioni per affermare come preponderante l'interesse del pubblico ad avere accesso, nel contesto di una ricerca *online*, alle informazioni personali, ritenendo prevalenti i diritti di cui agli artt. 7 e 8 della Carta, anche rispetto all'interesse economico del gestore del motore di ricerca, purché vi sia una verifica inerente al diritto dell'interessato, che potrebbe essere sacrificato nel caso in cui sussistano ragioni particolari (come il ruolo ricoperto nella vita pubblica) che giustifichino l'ingerenza nei suoi diritti fondamentali per la sussistenza di un interesse preponderante del pubblico ad ottenere l'informazione.

4. Tutela della riservatezza Versus interesse all'accertamento e alla prevenzione dei reati. Uno sguardo ai più recenti sviluppi in Europa

Il diritto all'oblio oltre a poter comportare una forte limitazione alla libertà di espressione, agli interessi economici dei *providers* e alla libertà di impresa, nonché all'interesse generale all'accertamento ed alla prevenzione di gravi reati per la tutela della riservatezza dell'individuo, può portare con sé i rischi di 'amnesia', temporanea o permanente, della rete.

Ciò non significa che l'informazione non sia più presente, in quanto potrebbe essere archiviata in specifici *data bases*, siti fonte, *servers* o in *cloud*. Essa comporta, però, oggettive difficoltà di raggiungimento di quei dati, che potrebbero tradursi nell'impossibilità, temporanea o permanente, di recuperarli se non viene individuata la 'fonte' o il 'luogo virtuale' di archiviazione. Una parte della dottrina straniera¹³ ha sostenuto che i *search engines* non devono essere considerati un valido sostituto alla stampa indipendente, ai casellari giudiziali o a rapporti o archivi storici.

Secondo questi autori sia gli individui che le organizzazioni che detengono un legittimo interesse in specifiche informazioni le possono ottenere tramite altri canali. Pertanto l'affidamento nei motori di ricerca è sopra valutato. Questa parte della dottrina, però, sottovaluta a sua volta che l'uso di quei canali presuppone la detenzione di alcune informazioni basilari da parte degli organi investigativi, che consenta di raggiungere la fonte del dato. In verità, l'indicizzazione di risultati in una ricerca *online* è utile proprio nella fase prodromica, ossia nel momento in cui difetta la conoscenza di dati preliminari che possano permettere la corretta

¹³ Vedi B. VAN ALSENOY, A. KUCZERAWY and J. AUSLOOS, *Search engines after Google Spain: internet@liberty or privacy@peril?*, cit., p. 72.

individuazione di tale fonte¹⁴.

Per l'accertamento e la prevenzione di reati, infatti, l'accesso a dati e informazioni personali comporta spesso un 'salto nel passato', per ricostruire trame comunicative, 'spostamenti' *online* e, talvolta, fisici, sulla scorta di tecniche di localizzazione. Il 'monitoraggio' della rete e, dunque, anche dei risultati della ricerca tramite *search tools* e *web search engine* può risultare in molti casi un'attività indispensabile al fine non solo di raccogliere elementi indiziari o probatori, ma anche per individuare la fonte o il luogo 'virtuale' specifico in cui sono 'archiviati' i dati. Si pensi, a titolo esemplificativo, alle attività di contrasto alla pedopornografia *online*, disciplinate in Italia dall'art. 14 l. n. 269/98, come modificata dalla l. n. 38/2006, oppure alla lotta al terrorismo, che si avvale in modo sempre più crescente di strumenti tecnologici o della rete.

In Germania, ad esempio, il § 5 co. 2, n. 11 del *Gesetz über den Verfassungsschutz in Nordrhein-Westfalen*, costituiva la base giuridica per definire la c.d. *Online Durchsuchung*¹⁵, che autorizzava un organismo di *intelligence* a 'protezione della Costituzione' (*Verfassungsschutzbehörde*) ad effettuare due tipi di misure d'indagine: in primo luogo, il monitoraggio e la ricognizione segreti di Internet e, in secondo luogo, l'accesso segreto a sistemi informatici.

¹⁴ Si consideri solo, a titolo esemplificativo, la possibilità, attraverso il motore di ricerca, di reperire un profilo utente in un social network, che potrebbe risultare estremamente utile a fini investigativi. Vedi a riguardo, nella letteratura italiana L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. merito*, fascicolo speciale, 12, 2012, pp. 2522 e ss.; nella letteratura spagnola: A. NIETO, M. MAROTO, *Redes sociales en internet y 'data mining' en la prospección e investigación de comportamientos delictivos*, paper, in UCLM (<http://www3.uclm.es>), 2010 [consultato il 30/09/2014]; nella letteratura tedesca e con risvolti pratici in materia di investigazioni, cfr. K. HOFFMANN, *Investigations on Social Networks. A German Perspective*, in *Eu crim*, 3/2012, pp. 137 e ss. Nella letteratura americana e anglo-sassone: J. P. SEMITSU, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, in 31 *Pace L. Rev.*, 2011, pp. 291 e ss.; M. O'FLOINN, D. ORMEROD, *Social Networking Sites, Ripa and Criminal Investigations*, in *Crim. Law Rev.*, 10, 2011, pp. 766- 789.

¹⁵ Vedi ampiamente, nella letteratura italiana, i primi commenti di R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 2009, pp. 695 ss., nonché a R. FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsuchung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention*, in *Cyberspazio e dir.*, 11, 2, 2010, pp. 359 ss. Nella letteratura tedesca basti il rinvio alle recenti monografie di D. KOHLMANN, *Online-Durchsuchungen und andere Massnahmen mit Technikeinsatz*, Baden Baden, 2012; W. ZIEBARTH, *Online-Durchsuchung*, Hamburg, 2013.

La Corte Costituzionale tedesca ha rilevato che la disciplina relativa all'uso di sistemi di 'sorveglianza' o di 'monitoraggio' dell'attività degli *users* deve rispettare i diritti fondamentali della persona, riconducibili all'art. 1, co. 1 *Grundgesetz* (GG) — la dignità umana è inviolabile ed il suo rispetto e la sua protezione costituiscono un dovere da parte delle autorità statali — all'art. 2, co. 1 GG — ogni individuo ha diritto al libero sviluppo della sua personalità, nella misura in cui non viola i diritti degli altri e l'ordine costituzionale o la legge morale — e, quali manifestazioni del diritto generale della personalità (*allgemeine Persönlichkeitsrecht*), all'art. 10 GG — *segretezza della corrispondenza e delle [tele]comunicazioni* (*Das Briefgeheimnis sowie das Postund Fernmeldegeheimnis sind unverletzlich*) — ed all'art. 13 GG — *inviolabilità del domicilio* (*Die Wohnung ist unverletzlich*).

In tal caso i giudici hanno evidenziato che vengono in rilievo due nuove forme di manifestazione di tradizionali diritti fondamentali: 1) il '*diritto di autodeterminazione informativa*' (*Recht auf informationelle Selbstbestimmung*), che va oltre la tutela della *privacy* e non si limita ad informazioni sensibili per loro natura, che conferisce alla persona, in linea di principio, il potere di determinare, in sé, la divulgazione e l'utilizzo dei suoi dati personali, anche se connotati da un contenuto informativo minimo, che amplia la tutela della libertà della vita privata in termini di diritti fondamentali;

2) il *diritto fondamentale alla garanzia della riservatezza e dell'integrità dei sistemi informatici*, in quanto i sistemi informatici oggetto di indagine possono contenere dati personali della persona in misura e diversità tali da facilitare la conoscenza di parti significative della sua vita o della sua personalità in ambiti sia privati che economico-professionali¹⁶.

In sintesi la Corte, pur avendo dichiarato incostituzionale la normativa del *Gesetz über den Verfassungsschutz in Nordrhein-Westfalen* — per il contrasto con i principi di chiarezza [precisione] e determinatezza (che trovano le basi negli artt. 20, 28, co. 1, GG), nonché con il principio di proporzionalità, il quale richiede che la compressione dei diritti fondamentali dovrebbe perseguire uno scopo legittimo ed essere idonea, necessaria ed opportuna quale mezzo per il raggiungimento di questo scopo — ha

¹⁶ Per la traduzione di alcuni essenziali parti della decisione vedi R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, cit., nonché a R. FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht*, cit. Si veda anche R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, cit.

ammesso, facendo espresso riferimento alla lotta al terrorismo, che la sicurezza dello Stato, come potere di garantire la pace e l'ordine costituzionali, e la sicurezza della popolazione da pericoli per la vita, l'incolumità fisica e la libertà, sono valori di rango costituzionale, che devono essere valutati e considerati nel bilanciamento con altrettanto alti valori e contro-interessi. Dalla motivazione della Corte appare evidente che la compressione dei diritti fondamentali nel contesto di *un obiettivo di prevenzione* soddisfa il requisito di adeguatezza solo se determinati fatti costituiscano un pericolo, nel singolo caso concreto, per un prevalente bene giuridico, benché possa non essere ancora accertato e non si possa quindi stabilire con sufficiente probabilità che il pericolo si concretizzerà in un prossimo futuro.

Con riferimento al c.d. 'monitoraggio' Giudici tedeschi hanno precisato che il diritto alla riservatezza ed integrità dei sistemi tecnologici di informazione, garantito dal diritto generale della personalità, non viene intaccato se il monitoraggio segreto di Internet è limitato ai dati che il titolare del sistema ha fornito tramite comunicazioni in Internet, in quanto tale soggetto ha, in termini tecnici, 'aperto' il suo sistema. In linea di principio, dunque, allo Stato non è negata la possibilità di ottenere informazioni accessibili al pubblico come, ad esempio, nel caso in cui raccolga dati e informazioni disponibili in Internet ed afferenti ad un gruppo di persone, anche tramite motori di ricerca¹⁷.

La stessa possibilità di effettuare un accesso segreto è costituzionalmente ammissibile solo se tale misura risulta essere necessaria per la protezione di *importanti e predominanti beni giuridici*, quali possono essere la vita, l'incolumità fisica e la libertà dei singoli, nonché quelli della collettività («*Güter der Allgemeinheit*»), la cui minaccia tocca le fondamenta dello Stato o il suo mantenimento o la base dell'esistenza umana, fino a comprendere anche la possibilità di funzionamento delle parti essenziali dei servizi di pubblica utilità. Purché le attività di indagine siano contro bilanciate da idonee precauzioni procedurali, riservando la misura ad un *ordine del giudice* che svolga un controllo preventivo, che dovrebbe avere la funzione di 'compensazione di rappresentanza' (*kompensatorischen Repräsentation*) degli interessi della persona interessata al procedimento.

Recentemente in Francia il Ministro dell'Interno Bernard Cazeneuve ha presentato una proposta di legge contro il terrorismo (il c.d. *Plan anti-jihad*) che dovrebbe rafforzare le misure preventive e di contrasto previste dalla *Loi* n. 2012-1432 del 21 dicembre 2012 «*relative à la sécurité et à*

¹⁷ Si pensi a strumenti come Archive-.org, che permette persino di reperire la cronostoria di domini Internet e siti e, in taluni casi, di navigare in versioni originarie, e risalenti nel tempo, di pagine Internet tramite un vero e proprio salto nel passato.

la lutte contre le terrorisme». Tale proposta prevede anche la possibilità di bloccare i siti Internet o oscurare le *web-pages* con contenuti atti all'apologia al terrorismo, al reclutamento o alla ricerca di finanziamenti, permettendo altresì all'autorità giudiziaria, nel corso di una ricerca, di recuperare dati e informazioni su *server* collocati all'estero, rendendo efficiente l'attività investigativa anche rispetto all'uso di nuove tecnologie come il *cloud*¹⁸.

In Olanda è stata proposta l'introduzione di uno strumento simile alla c.d. *Online Durchscheidung* tedesca, che consentirebbe alle autorità investigative, previa autorizzazione del giudice, di monitorare i sistemi informatici ed estrarre copia di dati, anche nel caso in cui non fosse possibile localizzare il *device*¹⁹. Anche in Spagna è stata proposta la modifica degli artt. 350, 351, 352 del *Código Procesal Penal*, al fine di disciplinare la possibilità di utilizzare un programma informatico in grado di accedere, all'insaputa dell'utente, ai dati contenuti in un sistema informatico, purché l'intervento avvenga per l'accertamento di un reato di particolare gravità e sia proporzionato, consentendo solo l'invasione necessaria ed indispensabile nei diritti fondamentali dell'individuo²⁰. Il Regno Unito dopo la sentenza della Corte di Giustizia sulla *data retention* ha adottato il «*Data retention and Investigatory Powers Act 2014*» che prevede la possibilità, tramite una retention notice emessa dal *Secretary State* di richiedere al *provider* di conservare, entro certi limiti, dati e informazioni, se necessari per prevenire o accertare reati, ovvero, fra gli altri presupposti, per la tutela della sicurezza nazionale, della sicurezza pubblica e della salute pubblica (v. sec. 22.2 *Regulation of Investigatory Powers Act 2000*). La nuova disposizione prevede i requisiti della *retention notice* e i rispettivi limiti. Il par. 5, però, fornisce una definizione molto ampia di 'telecommunications service', idonea a ricomprendere ogni servizio utile a facilitare la creazione, la gestione o l'archiviazione di comunicazioni che possono essere trasmesse tramite sistemi informatici (v. *Data retention and Investigatory Powers Act 2014* reperibile in <http://www.legislation.gov.uk>).

Se si volge lo sguardo all'Europa, con riferimento alla diffusione di materiale pedopornografico *online* il legislatore europeo, con la nuova direttiva in materia penale relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile²¹ ha previsto, all'art.

¹⁸ Il progetto di legge è reperibile in <http://www.gouvernement.fr/gouvernement/lutte-contre-le-terrorisme>.

¹⁹ Vedi quanto riportato da F. IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, 22 luglio 2014, pp. 1-20.

²⁰ Ibidem, a cui si rinvia anche per uno sguardo al sistema americano.

²¹ Direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei

15, co. 3, che gli Stati adottino tutte le misure necessarie per assicurare che le investigazioni, in questo settore, avvengano con mezzi adeguati ed effettivi, «al pari della lotta alla criminalità organizzata o ad altri gravi reati». Il successivo co. 4 dispone, inoltre, che gli Stati assicurino l'individuazione degli autori dei reati e delle vittime anche tramite l'analisi di immagini o prodotti audio video trasmessi o resi disponibili attraverso le tecnologie dell'informazione e della comunicazione. L'art. 25 della stessa direttiva prevede che gli Stati adottino le misure necessarie per assicurare la tempestiva rimozione delle pagine *web* contenenti immagini pedopornografiche, che abbiano *host* nel proprio territorio, ma con la possibilità di richiedere la stessa misura anche al di fuori dei limiti territoriali.

Gli Stati, inoltre, possono adottare misure di blocco di accesso degli utenti alle pagine web contenenti materiali pedopornografici. La direttiva dispone che tale strumento deve essere predisposto attraverso una procedura trasparente e prevedere delle *safeguards* per garantire che la restrizione sia limitata, necessaria e proporzionata, nonché il diritto dell'utente ad essere informato del motivo della restrizione. Tale procedura dovrebbe altresì garantire il ricorso giudiziario avverso al provvedimento che dispone il blocco dell'accesso.

In sintesi, si tratta di strumenti specifici predisposti per la lotta al fenomeno della pedopornografia *online*, adattabili alle esigenze repressive e preventive di tali attività criminose, che possono trovare proprio nei motori di ricerca gli 'alleati' indispensabili per un'azione tempestiva, efficace e con notevoli risparmi economici. In tutti questi casi siamo in presenza, sia a livello nazionale che a livello europeo, di innovativi mezzi di indagine a carattere tecnologico la cui regolamentazione e utilizzazione in concreto non può certo prescindere dal bilanciamento con altri interessi contrapposti, a partire dai diritti fondamentali dell'individuo. Dall'altro lato, però, essi dimostrano la necessità di sfruttare le potenzialità offerte dalle nuove tecnologie nella lotta non solo alla criminalità informatica, ma anche alla criminalità 'comune'²².

minori e la pornografia minorile (che sostituisce la decisione quadro 2004/68/ GAI) attuata in Italia con il d.lgs n. 39/2014.

²² Per una classificazione dei reati informatici e sulla definizione di criminalità informatica basti il rinvio, in questa sede, a L. PICOTTI, voce *Reati informatici*, in *Enc. giur.*, Agg., VIII, Roma, 2000, pp. 1 ss.; L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, pp. 21 ss.; L. PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec.*, 4, 2011, pp. 827 ss. Nella dottrina tedesca vedi U. SIEBER, *Computerkriminalität*, in U. SIEBER, F. H. BRÜNER, H. SATZGER, B. VON HEINTSCHEL-

Tale sfruttamento non può prescindere dal 'monitoraggio' della rete o dalla ricerca, tramite gli stessi *search engines*, di dati, utili anche solo a individuare la fonte dell'informazione personale, che potrebbe essere un nome di una persona associato ad un dominio, oppure inserito fra gli amministratori di un sito, fra i titolari del *copyright* di un prodotto o un'opera *online*, o fra i dipendenti di un'azienda o di un ente pubblico che pubblicano in rete i dati personali (anche solo nome e cognome) dei collaboratori.

5. La sentenza della Corte di Giustizia sulla c.d. data retention: un importante passo per il rafforzamento del diritto alla riservatezza. Ma con quali effetti per il sistema di giustizia penale?

In questo senso la sentenza della Corte di Giustizia sulla c.d. *data retention* ha notevolmente complicato la situazione²³.

I Giudici, infatti, hanno invalidato la direttiva 2006/24, in quanto non compatibile con i limiti imposti dal rispetto del principio di proporzionalità, alla luce degli artt. 7, 8 e 52, par. 1, della Carta. Tale direttiva richiedeva l'applicazione degli obblighi di conservazione a tutti i dati di traffico connessi a qualsiasi mezzo comunicativo. Questi obblighi riguardavano, dunque, l'archiviazione di dati relativi, in modo generalizzato, a tutti gli utenti e a tutti i mezzi di comunicazione elettronica, così come a tutte le modalità di traffico delle informazioni (via telefono, Internet, e-mail ecc.) senza differenziazioni, limiti o eccezioni rispetto all'obiettivo di contrastare la criminalità grave. Inoltre, tale archiviazione aveva ad oggetto dati di persone che, nemmeno indirettamente, si trovavano nella situazione di dare adito a procedimenti penali o di essere collegate, anche solo in modo remoto, a reati gravi, anche in situazioni in cui non sussistevano prove che la loro condotta potesse in qualche modo far sospettare

HEINEGG (Hrsg), *Europäisches Strafrecht*, Baden Baden, 2011, pp. 393 ss. Cfr. altresì R. FLOR, *Cybercriminality: Finding a Balance between Freedom and Security. An Introduction*, in S. Manacorda (ed.), R. Flor (coord.), J. Oh Jang (coord.), *Cybercriminality: Finding a Balance between Freedom and Security*, Milano, 2012, pp. 14 ss.

²³ Corte di Giustizia dell'Unione europea, sent. 8 aprile 2014 (C-293/12 and C-594/12), con commento di R. FLOR, *La corte di giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 28 aprile 2014, pp. 1-16, a cui si rinvia per l'approfondimento delle argomentazioni della Corte. Cfr., con riferimento agli effetti sia a livello europeo che nel sistema tedesco, S. NELLES, *Quo vadis Vorratsdatenspeicherung?*, Göttingen, 2014.

un loro coinvolgimento. Inoltre essa non prevedeva alcuna eccezione, con la conseguenza che si trovava ad essere applicata anche alle persone le cui comunicazioni erano soggette, in base alle norme di diritto nazionale, all'obbligo del segreto professionale.

La direttiva non prevedeva nemmeno alcun rapporto tra i dati oggetto dell'obbligo di conservazione e una minaccia per la sicurezza pubblica. In particolare, tale obbligo non era limitato a: *a)* dati relativi a un determinato periodo di tempo e/o una particolare zona geografica e/o ad un cerchio di persone che potevano essere coinvolte, in un modo o nell'altro, in un crimine grave; *b)* a persone che potevano, per altri motivi, contribuire, grazie alla conservazione dei loro dati, alla prevenzione, accertamento e perseguimento di reati gravi.

La direttiva non prevedeva nemmeno alcun limite oggettivo, sostanziale o procedurale²⁴, per l'accesso ai dati da parte delle competenti autorità nazionali e per il successivo utilizzo a fini di prevenzione, accertamento [o nell'ambito di procedimenti penali] riguardanti reati che, in considerazione della portata e della invasività della interferenza con i diritti fondamentali di cui agli artt. 7 e 8 della Carta, fossero di una gravità tale da giustificare una limitazione a questi diritti. Al contrario, la direttiva faceva riferimento in modo generale, *ex art.* 1, par. 1, a «reati gravi» come «definiti dagli Stati membri», e non prevedeva che l'accesso ai dati avvenisse dopo l'esame di un giudice o di una autorità amministrativa indipendente, la cui decisione potesse, a seguito di una richiesta motivata presentata nel quadro delle procedure di prevenzione o accertamento di gravi reati, o nell'ambito di procedimenti penali, limitare l'accesso ai dati e il loro utilizzo a quanto fosse strettamente necessario ai fini del raggiungimento dell'obiettivo perseguito. Per quanto riguarda il periodo di archiviazione dei dati, la direttiva faceva riferimento ad un lasso di tempo minimo (6 mesi) e massimo (24 mesi) senza distinguere le categorie di dati e la loro possibile utilità per il raggiungimento degli obiettivi perseguiti, ovvero in accordo con le persone coinvolte. Inoltre, il 'periodo finestra' non era basato su criteri oggettivi al fine di assicurare che fosse limitato alla stretta necessità. Ne conseguì che l'interferenza con i diritti fondamentali in esame avveniva senza limiti o regole precise.

Con riferimento alla sicurezza ed alla protezione dei dati oggetto dell'obbligo di archiviazione, la direttiva non prevedeva misure di garanzia sufficienti—come richieste, invece, dagli artt. 7 e 8 della Carta—in

²⁴ L'art. 4 della direttiva, infatti, lascia agli Stati membri il compito di definire le regole procedurali da seguire e i requisiti sostanziali per garantire l'accesso e la comunicazione dei dati.

specie contro il rischio di abusi, accesso illegale o uso non autorizzato, nonché in relazione alla molteplicità e diversità di dati che dovevano essere archiviati, alla natura dei medesimi ed ai rischi connessi alla loro integrità, confidenzialità e genuinità.

La direttiva, inoltre, non prevedeva l'obbligo per gli Stati membri di disciplinare elevati standard di sicurezza, permettendo in tal modo ai *providers* di poter seguire criteri di mera economicità per assicurare la protezione delle informazioni²⁵. Infine, la direttiva non richiedeva che i dati in questione dovessero essere conservati all'interno dell'Unione europea, con la conseguenza che non era possibile ritenere che il controllo, espressamente richiesto dall'art. 8, par. 3 della Carta, da parte di un'autorità indipendente in conformità con le esigenze di tutela e sicurezza dei dati, fosse pienamente garantito.

Leggendo a contrario questa sentenza è possibile ricavare alcune linee guida per una riforma della normativa sulla c.d. *data retention*.

Ferme le delicate questioni sui limiti temporali della conservazione dei dati e sulle procedure di accesso e di acquisizione delle informazioni, le criticità principali riguardano, *in primis*, l'individuazione dei 'gravi' reati 'presupposto', nonché la definizione dei presupposti oggettivi che possano giustificare la *data retention*.

In secondo luogo, la valutazione sull'esistenza di un *fumus commissi delicti* dovrebbe essere lasciata ad un organismo indipendente (giudice) attraverso la previsione di una procedura snella e 'tempestiva', che consenta comunque un accertamento concreto sulla sussistenza del reato 'presupposto', basato su elementi indiziari (provvedimento motivato dell'autorità giudiziaria su richiesta del pubblico ministero, anche su istanza del difensore dell'imputato), che può pervenire *ex post*, in un lasso di tempo comunque breve, esclusivamente in ipotesi di urgenza (ad esempio quando sussistono elementi oggettivi e concordanti relativi alla preparazione di attentati terroristici), purché vi sia una definizione: a) di un elevato livello delle 'misure di sicurezza' da adottare e delle procedure da seguire per la

²⁵ Il c.d. 'criterio di economicità' era già stato evidenziato, in senso critico, dalla Corte costituzionale tedesca nella citata sentenza del 2 marzo 2010 sulla *data retention* (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), on-line in http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html [consultato il 30/09/2014]. Per un primo commento in italiano si consenta il rinvio a R. FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchscheidung e la sua portata alla luce della sentenza del 2 marzo 2010 sul data retention*, in *Cyberspazio e diritto*, pp. 11, 2, 2010, 359-392. Nella letteratura tedesca vedi S. NELLES, *Quo vadis Vorratsdatenspeicherung?*, cit., pp. 265 ss.

conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento; *b*) di apposite sanzioni di inutilizzabilità del materiale probatorio acquisito in modo illecito o in caso di mancato rispetto del 'principio di necessità' nel trattamento dei dati (ad esempio quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato o le persone a lui collegate solo in caso di indispensabilità).

Se le norme interne dei singoli Stati, come nel caso italiano, non rispettano gli standard ricavabili dalla sentenza della Corte, esse dovrebbero essere disapplicate dal giudice interno per contrasto con il diritto europeo.

La soluzione più immediata, ma purtroppo ad effetto 'locale', vede come protagonista il legislatore nazionale, il quale dovrebbe intervenire ed adattare l'attuale disciplina agli standards elaborati dalla Corte di Giustizia.

Sarebbe però maggiormente auspicabile un intervento del legislatore europeo, nell'ambito di una più ampia politica criminale dell'Unione. La stessa individuazione dei fenomeni criminali gravi e di natura transnazionale, nonché la conseguente definizione dei 'reati presupposto', potrebbe trovare una base legale nell'art. 83, par. 1, del Trattato sul funzionamento dell'Unione europea (TFUE). Il *valore aggiunto* riguarda, da un lato, l'efficacia, per la forza vincolante delle fonti per gli Stati membri; dall'altro lato le *garanzie*, che devono circondare la produzione di norme penali (legittimazione democratica e trasparenza del procedimento legislativo, controllabilità politica, da parte dei Parlamenti nazionali durante la fase «ascendente» dei fondamentali principi di sussidiarietà europea e di proporzionalità, *ex* art. 5 TUE e Protocollo applicativo n. 2 allegato al TFUE, piena controllabilità giudiziaria di tali presupposti da parte della Corte di Giustizia ed, indirettamente, delle giurisdizioni nazionali nella fase applicativa). L'epocale sentenza della Corte di Giustizia, di cui si condivide l'iter argomentativo e motivazionale, che fonda le proprie basi nel percorso già intrapreso da numerose Corti costituzionali europee²⁶, si scontra con la complessità dell'attuale società dell'informazione, governata dalla inarrestabile rivoluzione informatica e dalla esasperata velocità evolutiva delle tecnologie, che hanno trasformato i dati e le informazioni in 'beni immateriali' di inestimabile valore.

Nell'attuale assetto sociale ed economico il ricorso a strumenti investigativi a 'contenuto tecnologico' e alla *data retention* risulta indispensabile,

²⁶ Vedi R. FLOR, *La Corte di Giustizia*, cit., pp. 1-16.

per prevenire e per accertare gravi reati lesivi di importanti beni giuridici²⁷.

Nella delicata operazione di bilanciamento fra le contrapposte esigenze di tutela, il c.d. 'diritto all'oblio', afferente alle prerogative della sfera di riservatezza della persona, deve essere considerato proprio rispetto all'interesse generale dell'accertamento e prevenzione di gravi reati.

I principi espressi dalle sentenze della Corte di Giustizia sui casi c.d. *data retention* e *Google/Spagna*, devono essere letti congiuntamente per tentare di elaborare una griglia di *standards* minimi per consentire tale giudizio di bilanciamento e per definire i contorni dei possibili limiti al diritto del soggetto interessato di ottenere la cancellazione dei dati e delle informazioni che lo riguardano anche da motori di ricerca.

6. Verso una definizione del 'diritto all'oblio'

6.1. Il diritto all'oblio nelle conclusioni dell'Avvocato Generale.

La ricostruzione del 'diritto all'oblio' effettuata dalla Corte di Giustizia nella sentenza *Google/Spagna* in parte contrasta con le conclusioni dell'avvocato generale, il quale ha affermato, sulla base di specifiche argomentazioni, che non possa ritenersi pacifico poter ricavare dalle norme della direttiva 95/46, interpretate alla luce delle disposizioni della Carta, un diritto 'generalizzato' all'oblio²⁸.

Secondo l'avvocato generale, infatti, *i diritti alla rettifica, alla cancellazione, al congelamento e all'opposizione previsti nella direttiva non corrispondano al «diritto all'oblio» della persona interessata*. In particolare la direttiva

²⁷ Gli stessi Stati membri, in generale, hanno affermato che la conservazione dei dati è «quanto meno utile, e in alcuni casi indispensabile, per prevenire e contrastare la criminalità, compresa la protezione delle vittime e l'assoluzione degli imputati innocenti». La Repubblica ceca, ad esempio, ha considerato la conservazione dei dati «assolutamente indispensabile in un gran numero di casi»; la Slovenia ha indicato che l'assenza di dati conservati «paralizzerebbe l'attività delle agenzie di contrasto»; l'Ungheria ha affermato che era «indispensabile nelle attività ordinarie [delle agenzie di contrasto]»; il Regno Unito ha descritto la disponibilità di dati relativi al traffico come «assolutamente essenziale ... per condurre indagini riguardanti il terrorismo e i reati gravi». Vedi in questo senso il rapporto della Commissione europea relativo alla «Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24)», COM(2011) 225 definitivo, p. 25, nota 105.

²⁸ Vedi, in questo senso, le conclusioni dell'Avvocato Generale Niilo Jääskinen presentate il 25 giugno 2013.

non prevederebbe un diritto generale di questo tipo che possa permettere al soggetto interessato di limitare o di impedire la diffusione di dati personali che egli consideri compromettenti o contrari ai propri interessi. I criteri da applicare dovrebbero invece essere individuati nello scopo del trattamento e negli interessi da questo tutelati, bilanciati con quelli della persona interessata, e non invece con le preferenze di quest'ultima. Pertanto, una preferenza soggettiva non dovrebbe costituire un motivo preminente e legittimo ai sensi dell'art. 14, lett. a), della direttiva 95/46.

Anche se il gestore del motore di ricerca è riconducibile alla categoria dei «responsabili del trattamento» (o, meglio, titolare/ *controller*), la persona interessata non avrebbe in ogni caso un «diritto all'oblio» assoluto da far valere. La sentenza della Corte affronta la questione del bilanciamento soprattutto rispetto alla tutela delle libertà di espressione e di impresa, seguendo la linea interpretativa della Corte europea dei diritti dell'uomo, la quale ha già dichiarato, nella sentenza Aleksey Ovchinnikov²⁹, che «in alcuni casi può essere giustificato limitare la riproduzione di informazioni già divenute di pubblico dominio, ad esempio al fine di impedire un'ulteriore diffusione dei dettagli della vita privata di una persona estranea a qualsiasi dibattito politico o pubblico su un argomento di importanza generale». Pertanto, in linea di principio, il diritto fondamentale alla protezione della vita privata può essere invocato anche se le informazioni di cui trattasi sono già di pubblico dominio.

Non ha torto l'Avvocato Generale quando sostiene che il problema della protezione dei dati si è posto, in questo caso, solo quando un utente ha inserito nome e cognome della persona interessata nel motore di ricerca ottenendo un *link* verso le pagine *web* di un giornale in cui compaiono gli articoli contestati. L'utente ha però *esercitato attivamente il proprio diritto ad ottenere informazioni relative alla persona interessata provenienti da fonti pubbliche* per motivi che possono essere fra i più disparati.

Cercare informazioni tramite motori di ricerca costituisce, nell'attuale contesto sociale, forse lo strumento più importante per esercitare tale diritto fondamentale.

Partendo da questa prospettiva, e considerando il legittimo diritto di impresa del fornitore dei servizi in Internet e del gestore del motore di ricerca, ossia quello di organizzare e indicizzare i risultati delle ricerche degli utenti, riconoscere valore predominante al diritto all'oblio vorrebbe dire sacrificare le libertà di espressione e di informazione, che potrebbero essere compromesse ulteriormente se la valutazione, caso per caso, fosse

²⁹ Aleksey Ovchinnikov v. Russia, n. 24061/04, 16 dicembre 2010.

lasciata solo alla decisione degli stessi fornitori di servizi.

In tale contesto, è condivisibile l'osservazione dell'Avvocato Generale, quando avverte che le «procedure di notifica e rimozione» di cui alla direttiva 2000/31 sul commercio elettronico si riferiscono a «contenuti illeciti, mentre il presente caso verte su una richiesta di soppressione di informazioni legittime e legali entrate nella sfera pubblica».

6.2. Il diritto all'oblio nella proposta di Regolamento europeo concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (Regolamento generale sulla protezione dei dati)

Il c.d. diritto all'oblio è espressamente disciplinato dall'art. 17 della Proposta della Commissione per un regolamento generale sulla protezione dei dati personali³⁰.

In estrema sintesi tale disposizione prevede il diritto all'oblio e alla cancellazione³¹, rafforzando il diritto alla cancellazione di cui all'art. 12,

³⁰ Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 def., 25 gennaio 2012.

³¹ Si riporta di seguito il testo dell'art. 17. «L'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati, in particolare in relazione ai dati personali resi pubblici quando l'interessato era un minore, se sussiste uno dei motivi seguenti: *a*) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; *b*) l'interessato revoca il consenso su cui si fonda il trattamento, di cui all'articolo 6, paragrafo 1, lettera *a*), oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattare i dati; *c*) l'interessato si oppone al trattamento di dati personali ai sensi dell'articolo 19; *d*) il trattamento dei dati non è conforme al presente regolamento per altri motivi. 2. Quando ha reso pubblici dati personali, il responsabile del trattamento di cui al paragrafo 1 prende tutte le misure ragionevoli, anche tecniche, in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Se ha autorizzato un terzo a pubblicare dati personali, il responsabile del trattamento è ritenuto responsabile di tale pubblicazione. 3. Il responsabile del trattamento provvede senza ritardo alla cancellazione, a meno che conservare i dati personali non sia necessario: *a*) per l'esercizio del diritto alla libertà di espressione in conformità dell'articolo 80; *b*) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 81; *c*) per finalità storiche, statistiche e di ricerca scientifica in conformità dell'articolo 83; *d*) per adempiere un obbligo legale di conservazione di dati personali previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento; il diritto dello Stato membro deve

lett. *b*) direttiva 95/46, nonché l'obbligo per il responsabile (titolare) del trattamento che abbia divulgato dati personali di informare i terzi della richiesta dell'interessato di cancellare tutti i link verso tali dati, le loro copie o riproduzioni.

La disposizione prevede inoltre il diritto di limitare il trattamento in determinati casi, evitando l'ambiguo termine di 'blocco dei dati'. In particolare, l'interessato deve avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o trattati, quando abbia ritirato il consenso o si sia opposto al trattamento o quando questo ultimo non sia conforme alle disposizioni del regolamento. Tuttavia, occorre consentire l'ulteriore conservazione dei dati qualora sia necessario per finalità storiche, statistiche e di ricerca scientifica, per motivi di interesse pubblico nel settore della sanità pubblica, per l'esercizio del diritto alla libertà di espressione, ove richiesto per legge o quando sia giustificata una limitazione del trattamento dei dati anziché una loro cancellazione.

Per garantire tale informazione, è necessario che il responsabile (titolare) del trattamento prenda tutte le misure ragionevoli, anche di natura tecnica, in relazione ai dati della cui pubblicazione è responsabile, anche

perseguire un obiettivo di interesse pubblico, rispettare il contenuto essenziale del diritto alla protezione dei dati personali ed essere proporzionato all'obiettivo legittimo; *e*) nei casi di cui al paragrafo 4. 4. Invece di provvedere alla cancellazione, il responsabile del trattamento limita il trattamento dei dati personali: *a*) quando l'interessato ne contesta l'esattezza, per il periodo necessario ad effettuare le opportune verifiche; *b*) quando, benché non ne abbia più bisogno per l'esercizio dei suoi compiti, i dati devono essere conservati a fini probatori; *c*) quando il trattamento è illecito e l'interessato si oppone alla loro cancellazione e chiede invece che ne sia limitato l'utilizzo; *d*) quando l'interessato chiede di trasmettere i dati personali a un altro sistema di trattamento automatizzato, in conformità dell'articolo 18, paragrafo 2. 5. I dati personali di cui al paragrafo 4 possono essere trattati, salvo che per la conservazione, soltanto a fini probatori o con il consenso dell'interessato oppure per tutelare i diritti di un'altra persona fisica o giuridica o per un obiettivo di pubblico interesse. 6. Quando il trattamento dei dati personali è limitato a norma del paragrafo 4, il responsabile del trattamento informa l'interessato prima di eliminare la limitazione al trattamento. 7. Il responsabile del trattamento predispone i meccanismi per assicurare il rispetto dei termini fissati per la cancellazione dei dati personali e/o per un esame periodico della necessità di conservare tali dati. 8. Quando provvede alla cancellazione, il responsabile del trattamento si astiene da altri trattamenti di tali dati personali. 9. Alla Commissione è conferito il potere di adottare atti delegati in conformità all'articolo 86 al fine di precisare: *a*) i criteri e i requisiti per l'applicazione del paragrafo 1 per specifici settori e situazioni di trattamento dei dati; *b*) le condizioni per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico, come previsto al paragrafo 2; *c*) i criteri e le condizioni per limitare il trattamento dei dati personali, di cui al paragrafo 4».

se ha autorizzato un terzo a pubblicarli.

Anche nei casi in cui i dati personali possano essere lecitamente trattati per proteggere interessi vitali dell'interessato, oppure per motivi di pubblico interesse, nell'esercizio di pubblici poteri o per il legittimo interesse di un responsabile (titolare) del trattamento, l'interessato deve comunque avere il diritto di opporsi al trattamento dei dati che lo riguardano.

La proposta di regolamento, però, prevede specifiche limitazioni al diritto all'oblio e alla cancellazione dei dati, fornendo una base giuridica per il bilanciamento fra contrapposte esigenze, ancorata al rispetto del principio di legalità. L'art. 21, infatti, dispone che l'Unione o gli Stati membri possono limitare, mediante misure legislative, la portata di tale diritto qualora la limitazione costituisca una misura necessaria e proporzionata in una società democratica per salvaguardare: *a)* la pubblica sicurezza; *b)* le attività volte a prevenire, indagare, accertare e perseguire reati; *c)* altri interessi pubblici dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, e la stabilità e l'integrità del mercato; *d)* le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; *e)* una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lett. *a)*, *b)*, *c)*, e *d)*; *f)* la tutela dell'interessato o dei diritti e delle libertà altrui.

La questione più delicata riguarda l'individuazione dell'organo o del soggetto deputato al giudizio di bilanciamento fra le diverse esigenze, da un lato, di tutela della riservatezza e, dall'altro lato, di giustizia penale o per la tutela della sicurezza pubblica o, ancora, per la protezione della libertà di espressione.

L'art. 12 della proposta di regolamento fa incombere in prima battuta sul responsabile (titolare) del trattamento l'obbligo di stabilire le procedure per l'esercizio dei diritti dell'interessato, fra i quali quelli di cui all'art. 17, che devono comprendere l'informazione a tale soggetto, tempestivamente e al più tardi entro un mese — termine prorogabile in casi specifici (se più interessati esercitano i loro diritti e la loro cooperazione è necessaria in misura ragionevole per evitare un impiego di risorse inutile e sproporzionato al responsabile del trattamento dal ricevimento della richiesta) — se è stata adottata un'azione. Se il responsabile (titolare) rifiuta di ottemperare alla richiesta dell'interessato, egli deve informarlo dei motivi e delle possibilità di proporre reclamo all'autorità di controllo e anche ricorso giurisdizionale.

È noto che nella maggior parte dei casi il fornitore di servizi è un soggetto privato che esercita la libertà di impresa. Egli dovrebbe dimostrare, in caso di rifiuto, non solo che i suoi legittimi interessi possono prevalere sull'interesse o sui diritti e sulle libertà fondamentali dell'interessato, ma anche che la richiesta, nel settore che qui interessa, non possa essere accolta per le esigenze legate alle attività volte a prevenire, indagare, accertare e perseguire reati. La proposta di regolamento, però, non individua espressamente un nucleo di reati gravi, che possano giustificare un'invasione nella sfera di riservatezza dell'individuo o, quantomeno, la necessità di proteggere beni giuridici di predominante importanza.

Inoltre, il fornitore di servizi coinvolto attivamente in attività di indagine svolge un ruolo di carattere 'pubblico', che comporta in molti casi il riserbo sulla natura del coinvolgimento o sull'attività che è 'delegato' a svolgere per gli organi investigativi. Egli sarà dunque portato a rifiutare la cancellazione dei dati o il pieno esercizio del diritto all'oblio, lasciando all'autorità di controllo o all'autorità giudiziaria giudicare su eventuali reclami.

La proposta di regolamento, però, prevede, *ex art. 79*, specifiche sanzioni amministrative nel caso in cui il responsabile (titolare) non rispetti il diritto all'oblio o alla cancellazione, ometta di predisporre meccanismi che garantiscano il rispetto dei termini o non prenda tutte le misure necessarie per informare i terzi della richiesta dell'interessato di cancellare tutti i link verso i dati personali, copiare tali dati o riprodurli, in violazione dell'*art. 17*, salve le ulteriori sanzioni, che potrebbero avere altresì natura penale, previste dagli Stati membri, *ex art. 78* della stessa proposta.

A ciò si aggiungono gli obblighi generali previsti dall'*art. 22* della proposta, fra cui quelli inerenti alla sicurezza dei dati, disciplinati dal successivo *art. 30*.

In conclusione, il diritto all'oblio definito dalla nuova proposta non è di natura assoluta e omnicomprensivo dei diritti riconosciuti al soggetto interessato.

7. Verso una definizione 'integrata' del diritto all'oblio e possibili linee guida per il bilanciamento con le esigenze proprie del sistema di giustizia: fra proposte de jure condendo e prospettive de jure condito

A questo punto, e ai fini del presente lavoro, non rimane che affrontare

la questione relativa ai rapporti fra diritto all'oblio ed esigenze di perseguire, accertare o prevenire gravi reati, che presuppone la lettura integrata fra le sentenze della Corte di Giustizia sulla *data retention* e sul caso Google/Spagna.

In prospettiva *de jure condendo*, considerando la proposta di regolamento europeo, nella sua attuale formulazione, si potrebbe delimitare il c.d. diritto all'oblio, anche nell'ottica di una auspicabile disciplina degli obblighi di archiviazione dei dati di traffico telefonico e telematico.

Dovrebbe però essere prevista la possibilità di cancellare o rimuovere i dati personali, su richiesta del soggetto interessato, in particolare dai motori di ricerca, dopo un periodo — finestra determinato, in cui eventualmente tali informazioni dovrebbero essere rese non accessibili al pubblico o alle persone non autorizzate.

In tal caso il legislatore europeo, alla luce delle citate sentenze della Corte, dovrebbe osservare le linee guida ricavabili dalla decisione sulla c.d. *data retention* e predisporre un 'sistema di obblighi integrato', che preveda: limiti temporali alla conservazione dei dati; procedure di accesso e di acquisizione delle informazioni; l'individuazione dei 'gravi' reati 'presupposto', nonché la definizione dei presupposti oggettivi che possano giustificare la *data retention*; che la valutazione sull'esistenza dei presupposti sia lasciata ad un organismo indipendente (giudice) attraverso la previsione di una procedura snella e 'tempestiva', purché vi sia una definizione *a)* di un elevato livello delle 'misure di sicurezza' da adottare e delle procedure da seguire per la conservazione, l'estrazione e, eventualmente, la cancellazione dei dati al termine del procedimento o del trattamento; *b)* di apposite sanzioni di inutilizzabilità del materiale probatorio acquisito in modo illecito o in caso di mancato rispetto del 'principio di necessità' nel trattamento dei dati.

A questi presupposti dovrebbero aggiungersi gli obblighi di rendere inaccessibili i dati, su richiesta del soggetto interessato. In tal caso si tratterebbe di un diritto all'oblio bifasico. In una prima fase l'interessato otterrebbe l'effetto di non rendere accessibili le informazioni (ad esempio tramite motori di ricerca o i siti che le contengono), le quali però, sul piano tecnico, rimarrebbero a disposizione del fornitore del servizio-se il soggetto destinatario dell'obbligo è riconducibile a questa categoria-per un periodo limitato, utile e necessario per il perseguimento, l'accertamento o la prevenzione di gravi reati. In tal caso sarebbe possibile il coordinamento fra la proposta di regolamento europeo, in particolare l'art. 21, con una futura e auspicabile disciplina europea in materia di *data retention*.

In una seconda fase, ossia trascorso il periodo previsto da tale ultima disciplina, il fornitore del servizio potrebbe procedere alla cancellazione del dato, salve le ulteriori esigenze di proroga della conservazione nel caso in cui il soggetto interessato sia divenuto indagato o imputato in un procedimento penale. In tale ultima situazione potrebbe trovare piena applicazione una disposizione quale quella di cui all'art. 21 della proposta di regolamento. La qualità di indagato o imputato, infatti, giustificerebbe la conservazione di dati anche con riferimento ai reati non inclusi in un'ipotetica lista di incriminazioni presupposto di una certa gravità.

Per quanto riguarda gli aspetti 'procedurali', un primo modello potrebbe essere ricavato dalla direttiva *e-commerce* e basarsi su un procedimento ingiunzionale connotato da un atto qualificato di un organismo indipendente (un giudice, anche eventualmente su segnalazione o su richiesta della persona fisica o dell'autorità garante), in modo da consentire di effettuare il bilanciamento fra le contrapposte esigenze di tutela e di perseguimento di interessi generali collettivi, che non può essere lasciato all'apprezzamento 'soggettivo' del singolo *provider*³². Tale 'modello' troverebbe conferma sia nella sentenza della Corte sulla *data retention*³³ sia in quella sul caso Google/Spagna³⁴.

La 'gravità potenziale' dell'ingerenza nei diritti fondamentali verrebbe via via affievolita proprio in base alla rilevanza dei contro interessi e dei diritti che necessiterebbero di tutela quantomeno paritaria. A ciò deve aggiungersi che a favore della non cancellazione possono sussistere, in primo luogo, anche ragioni statali tipiche di natura paternalistica, ossia quando i dati sono raccolti ed archiviati nell'interesse del medesimo indi-

³² Si vedano i rilievi critici espressi da R. FLOR, *La Corte di Giustizia*, cit.

³³ Vedi *supra*, par. 5.

³⁴ Vedi punto 82 della sentenza: «L'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di applicazione degli artt. 12, lett. b), e 14, co. 1, lett. a), della direttiva 95/46, da effettuarsi allorché ricevono una domanda quale quella oggetto del procedimento principale, possono ordinare al suddetto gestore di sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona, senza che un'ingiunzione in tal senso presupponga che tale nome e tali informazioni siano, con il pieno consenso dell'editore o su ingiunzione di una delle autorità sopra menzionate, previamente o simultaneamente cancellati dalla pagina web sulla quale sono stati pubblicati». Ex art. 28, par. 3 e 4 della direttiva, qualsiasi persona può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali, e che tale autorità dispone di poteri investigativi e di poteri effettivi di intervento che le consentono di ordinare in particolare il congelamento, la cancellazione o la distruzione di dati, oppure di vietare a titolo provvisorio o definitivo un trattamento.

viduo e/o della collettività. In tal caso, pur potendo limitare l'accesso a queste informazioni, esse non dovrebbero essere completamente eliminate ma solamente, e eventualmente, oscurate (*rectius* rese accessibili solo a persone determinate, autorizzate o legittimate). In secondo luogo, possono prevalere non solo interessi collettivi o generali, che portano beneficio all'intera comunità, come nel caso delle esigenze legate alla repressione e alla prevenzione dei reati, nonché alla raccolta della prova in formato digitale, che rispondono altresì all'esigenza di proteggere la sicurezza nazionale, ma anche, come ha affermato la Corte di Giustizia, la libertà di espressione e la libertà economica³⁵.

Fermo restando il diritto del soggetto interessato di ottenere, tramite l'ordine di un giudice, la cancellazione di dati o informazioni che lo riguardano, che costituiscono gli 'effetti' o il 'pregiudizio' di un illecito già accertato (si pensi ai classici casi di diffamazione tramite *social networks*, blog o siti indicizzati dai motori di ricerca: in questo caso l'interesse principale della 'vittima' è ottenere la rimozione della notizia diffamatoria dai risultati delle ricerche *online* e/o dai siti in cui si trova³⁶).

³⁵ In questo senso vedi P. BERNAL, *Internet Privacy Rights*, Cambridge University Press, 2014, pp. 199 ss. È utile tenere distinta la figura di un motore di ricerca rispetto a quella di siti-fonte o testate giornalistiche online. Il trattamento da parte dell'editore di una pagina *web*, infatti, potrebbe consistere nella pubblicazione di informazioni relative a una persona fisica, effettuata «esclusivamente a scopi giornalistici». *Ex art. 9* della direttiva 95/46, egli beneficerebbe delle deroghe alle prescrizioni dettate da quest'ultima, mentre non integrerebbe tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca. Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli artt. 12, lett. *b*), e 14, co. 1, lett. *a*), della direttiva contro il suddetto gestore del motore di ricerca, ma non contro l'editore della pagina *web*.

³⁶ Si veda a titolo esemplificativo, fra alcuni dei più recenti casi italiani: Trib. Milano, ord. 24 marzo 2011. Si veda altresì la recente proposta di legge «Modifiche alla legge 8 febbraio 1948, n. 47, al codice penale e al codice di procedura penale in materia di diffamazione, di diffamazione con il mezzo della stampa o con altro mezzo di diffusione, di ingiuria e di condanna del querelante» (Atto Camera 925 - Atto Senato 1119), in particolare nella versione emendata a seguito della sentenza della Corte di Giustizia sul caso Google/Spagna: «Art. 2-bis (*Misure a tutela del soggetto diffamato o del soggetto leso nell'onore e nella reputazione*) 1. Fermo restando il diritto di ottenere la rettifica o l'aggiornamento delle informazioni contenute nell'articolo ritenuto lesivo dei propri diritti, l'interessato può chiedere ai siti internet e ai motori di ricerca l'eliminazione dei contenuti diffamatori o dei dati personali trattati in violazione delle disposizioni di cui alla presente legge. 2. L'interessato, in caso di rifiuto o di omessa cancellazione dei dati, ai sensi dell'articolo 14 del decreto legislativo 9 aprile 2003, n. 70, può chiedere al giudice di ordinare ai siti internet e ai motori di ricerca la rimozione delle immagini e dei dati ovvero di inibirne l'ulteriore diffusione. 3. In caso di morte dell'interessato, le facoltà e i diritti di cui al comma 2 possono essere esercitati dagli

Analogamente, come è ricavabile dalle motivazioni della sentenza nel caso Google/Spagna, dovrebbe rimanere fermo il diritto all'oblio dell'autore di un reato che, scontata la pena, vede associato il proprio nome a fenomeni criminosi anche a distanza di molti anni, nel rispetto degli standard e dei meccanismi procedurali descritti dalla Corte stessa, eventualmente integrati con le ulteriori safeguards sopra riportate³⁷.

Ad ogni modo la domanda della persona interessata presuppone l'incompatibilità con la direttiva 95/46 del trattamento, anche se questo inizialmente era da considerarsi lecito³⁸.

8. Conclusioni

Nell'attuale assetto della società dell'informazione e di Internet non è possibile pensare di affrontare le sfide poste dalle nuove tecnologie senza poter sfruttare le loro potenzialità. La questione da porsi riguarda i limiti entro i quali può operare il legislatore (nazionale ed europeo) nella compromissione dei diritti fondamentali e nel prevedere gli standards su cui basare il delicato giudizio di bilanciamento con altri diritti fondamentali e con le esigenze di tutelare importanti interessi generali e collettivi, nel rispetto del principio di proporzione. Al riguardo, l'art. 52 della Carta dei diritti fondamentali dell'Unione europea, identifica proprio nel principio di proporzione il criterio guida fondamentale, sia sul piano ermeneutico che su quello delle scelte politico normative del legislatore, delimitandone l'area di discrezionalità. Le sfide lanciate da nuovi fenomeni illeciti o di natura criminosa, nonché le esigenze di prevenzione ed accertamento dei reati, richiedono un percorso di scelte che non è paragonabile al viaggio di Raffaele Itlodeo nell'isola di *Utopia*, una *societas perfecta*³⁹.

Sarebbe utopistico, infatti, credere che l'utente medio del nuovo millennio non utilizzi le opportunità offerte dalla evoluzione-rivoluzione informatica. Sarebbe altrettanto utopistico credere di contrastare forme di criminalità anche grave senza ricorrere alle stesse opportunità offerte

eredi o dal convivente».

³⁷ Vedi *supra*, par. 2 e 3.

³⁸ Con il tempo, infatti, tale trattamento potrebbe non essere più necessario in rapporto alle finalità per le quali sono stati raccolti i dati, come nei casi in cui essi risultino inadeguati, o non siano più pertinenti, in rapporto proprio al tempo trascorso.

³⁹ Cfr. T. MORE, *Libellus vere aureus, nec minus salutaris quam festivus de optimo rei publicae statu, deque nova insula Utopia*, p. 1516.

dalla evoluzione-rivoluzione informatica. Per queste ragioni le linee guida ricavabili dalla lettura sistematica delle sentenze della Corte di Giustizia sui casi Google/ Spagna e *data retention* potrebbero costituire il primo ed importante mattone delle fondamenta su cui edificare i 'parametri' certi per consentire il giudizio di bilanciamento fra le contrapposte esigenze di tutela, nonché di accertamento e prevenzione dei reati. Nella consapevolezza che «*chi controlla il passato, controlla il futuro; chi controlla il presente, controlla il passato*»⁴⁰ e che il passato non esiste solo nei documenti o nella memoria degli uomini, ma sempre più nella rete.

Abstract

The recent judgment of the European Court of Justice on the s.c. «Google/ Spain case» has recognised the «right to be forgotten».

But the right to privacy, in general, must be balanced with the protection of other fundamental rights (like freedom of expression and information and freedom to conduct a business) and important collective interests (like prevention, investigation, detection and prosecution of criminal offences).

The principles laid down by this decision should be read in a broad context, taking into account the judgement of the Court of Justice on the «data retention case».

The aim of this paper is to provide common standards, resulting from these judgements, in order, on the one hand, to define the limits of the right to be forgotten and the right to privacy and, on the other hand, to pursue the general interests of the criminal justice system, respecting fundamental rights by a balance based on those standards.

⁴⁰ G. ORWELL, 1984, cit

Franco Pizzetti

*Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il 'Velo di Maya'*¹

SOMMARIO: 1. La decisione Google Spain e le Autorità garanti - 2. La domanda di pronuncia pregiudiziale sottoposta alla Corte e la legittimità della richiesta di deindicizzazione dai motori di ricerca - 3. I singoli quesiti interpretativi affrontati nella decisione - 3.1. La qualificazione della attività svolta dai motori di ricerca - 3.2. Il gestore del motore di ricerca come titolare dei trattamenti — 3.3. Il principio di stabilimento e la sua applicabilità ai motori di ricerca - 3.4. La legittimità della richiesta di deindicizzazione e il combinato disposto art. 14 primo comma lettera *a*) e art. 7 lettere *e*) e *f*) della Direttiva - 3.5. Il punto essenziale: il diritto dell'interessato alla de-indicizzazione prevale di massima sull'interesse del gestore e su quello degli utenti - 3.6. Il diritto degli utenti all'informazione come limite al diritto dell'interessato, condizionato all'esistenza di situazioni specifiche - 4. Il 'nociolo duro' della decisione - 5. A proposito di alcune censure espresse dalla dottrina - 6. La eccessiva genericità dei criteri indicati al punto 97 della sentenza relativamente al limite all'accogliibilità della richiesta. I condizionamenti posti dalla Direttiva e i nodi non sciolti dal nuovo Regolamento. Verso un 'procuratore ai dati'? - 7. Quale il ruolo delle Autorità dopo la decisione Google Spain e nella realtà della rete? È tempo di far cadere il velo di Maya

1. La decisione Google Spain e le Autorità garanti

Il caso Google Spain e la sentenza della Corte di giustizia (Grande Sezione) del 13 maggio 2014 sono stati oggetto in questi mesi non solo di una grande campagna mediatica, legata essenzialmente alla magica, quanto ambigua, espressione 'diritto all'oblio' e alle suggestioni che essa evoca, ma anche di un importante dibattito scientifico che durerà certamente ancora a lungo. Il caso è noto, ed è ricostruito con ampiezza, e dai più diversi punti di vista, nei saggi raccolti in questo Volume. È possibile dunque limitarsi a sottolineare solo gli aspetti di maggior rilievo della decisione, sia per individuarne il contenuto sostanziale e, quindi, esaminarne

¹ Il primo a parlare del Velo di Maya come della illusione che vela tutte le cose fu A. Schopenhauer nel *«Il mondo come volontà e rappresentazione»*, 1819; La necessità di stracciare il Velo di Maya fu invece teorizzata da F. Nietzsche, *«La Nascita della tragedia»*, 1872.

meglio anche gli effetti, sia per mettere in luce i problemi e le sfide che essa pone alle Autorità garanti.

Non vi è dubbio, infatti, che la circostanza stessa che tutta la decisione sia formalmente basata sull'interpretazione e l'applicazione della Direttiva 95/46 del 24 ottobre 1995 «relativa alle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati» invoca il ruolo e la competenza delle Autorità di garanzia sia a livello nazionale (art. 28 direttiva), che riunite nel Working Party 29 (art. 29). Innanzitutto la decisione della Corte del Lussemburgo affida ad esse il compito di intervenire, in alternativa agli organi giurisdizionali degli Stati, in caso di ricorso dell'interessato non soddisfatto della risposta ricevuta dal motore di ricerca alla sua richiesta di cancellazione (deindicizzazione) dei suoi dati. In secondo luogo tocca ora proprio a queste Autorità dare anche in modo proattivo, ai provider, agli interessati e agli utenti della rete (e in particolare dei motori di ricerca) le indicazioni e raccomandazioni necessarie a garantire una attuazione per quanto possibile uniforme e condivisa della pronuncia della Corte di Giustizia². Si tratta, infatti, di una decisione che non manca di lasciare in più punti elementi di incertezza che potrebbero condurre, in assenza di idonee indicazioni, a interpretazioni e attuazioni tra loro difformi e persino contrapposte. Lo stesso dibattito scientifico che si è sviluppato in questi mesi già dimostra quanto questo pericolo sia reale e quanto diverse siano le letture che possono essere date di questa sentenza e dei suoi effetti. Non a caso del resto le Autorità garanti europee, che peraltro hanno già preso in esame per ben tre volte questa decisione³, anche avviando una discussione per ora interna al WP29 e

² Coglie perfettamente questo aspetto il Segretario generale dell'autorità garante per la protezione dei dati personali G. BUSIA, *Una vera rivoluzione copernicana*, in *Quotidiano del diritto*, 13 maggio 2014.

³ Una prima volta le Autorità sono intervenute col comunicato stampa del 23 maggio, nel quale, sottolineando che la decisione della Corte dà risposte innovative e importanti in ordine al concetto di stabilimento, di trattamento dei dati e di titolarità, applicati alle attività di indicizzazione dei dati personali da parte dei motori di ricerca, e compiacendosi che si fosse stabilita la applicabilità della direttiva e il diritto dell'interessato di chiedere direttamente al gestore la cancellazione (deindicizzazione) dei suoi dati, raccomandavano attenzione nel valutare caso per caso la sussistenza di tale diritto. In un secondo comunicato stampa, del 6 giugno, le Autorità hanno reso noto di aver avviato una discussione al loro interno (a quel che risulta piuttosto articolata), promuovendo anche una audizione di Google e di altri motori di ricerca. Infine, in un terzo comunicato del 25 luglio, il WP29 ha dato notizia di aver sentito Google, Microsoft e Yahoo!, ponendo domande specifiche e chiedendo ad essi di rispondere per lettera entro il 31 luglio a una serie di domande, peraltro rese note in quello stesso comunicato. Nel medesimo comunicato, il WP29 si riservava inoltre di organizzare altri incontri e annunciava l'intenzione di appro-

tenendo audizioni interlocutorie, hanno già annunciato per il prossimo autunno l'adozione di una decisione organica e strutturata, che probabilmente assumerà anche la forma di 'linee guida'⁴.

2. La domanda di pronuncia pregiudiziale sottoposta alla Corte e la legittimità della richiesta di de-indicizzazione dai motori di ricerca

La sentenza, come tutte le sentenze, è incentrata sulla questione proposta alla Corte. Questa questione, vale la pena ricordarlo, è una domanda di pronuncia pregiudiziale proposta ai sensi dell'art. 267 TFUE, dall'*Audiencia Nacional* (Spagna) con decisione del 27 febbraio 2012⁵.

La domanda verte esplicitamente sull'interpretazione da dare agli art. 2 lettera b) e d), 4 paragrafo 1 lettere a) e c), 12 lettera b) e 14 primo comma lettera a) della direttiva 95/46 CE del 1995, nonché dell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea.

Essa è stata posta nell'ambito di una controversia tra la società Google Spain e Google Inc., da un lato, e l'*Agencia Espanola de Protección de Datos* e il sig. Costeja Gonzales, dall'altro, in merito a una decisione della *Agencia* che aveva accolto la denuncia depositata dal sig. Costeja Gonzales contro le due società per ottenere la deindicizzazione di alcuni dati personali che lo riguardavano e impedirne l'accesso nel futuro.

Dunque la domanda di pronuncia pregiudiziale non ha al centro il 'diritto all'oblio', categoria talora mediatica e, solo in parte, scientifica e normativa⁶, e che avrebbe comportato il sorgere di problemi importanti e

vare apposite Linee guida entro l'autunno. Linee guida che peraltro sono state chieste da più parti e in particolare dal *Center for democracy and technology*, con una lettera del suo Presidente Nuala O'Connor, inviata il 25 luglio al Presidente della CNIL e del WP29 Isabelle Falque-Pierrotin.

⁴ Nelle more della pubblicazione di questo lavoro il WP29, nella riunione del 17-18 settembre, ha preso in esame alcune proposte di Linee Guida formulate dal gruppo di lavoro interno. Per il momento ha però deciso di creare un «*common toolbox*» per raccogliere ulteriori elementi comuni e per monitorare le richieste pervenute ai provider e gli esiti relativi. Cfr. *Press Release* del WP29, in data 18 settembre 2014.

⁵ La domanda di pronuncia pregiudiziale della *Audiencia Nacional* spagnola era già stata oggetto di numerosi dibattiti prima della attuale decisione della Corte di Giustizia e anche prima che l'Avvocato generale esprimesse le sue conclusioni. Su questo punto, anche con riguardo al dibattito sul diritto all'oblio in rete e al futuro Regolamento europeo si veda tra gli altri M. SIANO, *Il diritto all'oblio in Europa e il recente caso spagnolo*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, Giappichelli, Torino, 2013.

⁶ Sul diritto all'oblio v. per tutti la eccellente ricostruzione e le acute riflessioni di G.

difficili, legati alla contrapposizione ad altri diritti non meno fondamentali per la società, come il diritto all'informazione (cioè a informare e a essere informati); il diritto alla manifestazione del pensiero; il diritto alla memoria (cioè alla conservazione e tutela delle tracce del passato da proteggere e conservare anche, e soprattutto, per le nuove generazioni).

Caso mai, considerando che al centro di tutta la vicenda vi è la richiesta del sig. Costeja Gonzales a Google di cancellazione (deindicizzazione) di taluni dati personali che lo riguardano riferiti a un antico episodio reso pubblico a suo tempo dal giornale *La Vanguardia*, al quale peraltro non viene richiesta alcuna cancellazione dal suo sito, si potrebbe parlare, come si è fatto, di «diritto a non essere facilmente trovato»⁷.

È evidente infatti che se si chiede la deindicizzazione al motore di ricerca ma non la cancellazione da ogni altro sito, e in particolare dal sito-sorgente, non si intende affatto far vale un diritto all'oblio, che non c'è e comunque in questo caso, con questa richiesta, sarebbe di dubbia attivazione, ma caso mai il diritto a non vedere facilmente trovata una notizia non più attuale. L'effetto principale della indicizzazione e diffusione delle notizie attraverso il motore di ricerca è infatti quello di concorrere in modo continuo a riattualizzare tutte le informazioni, facendole diventare tutte elementi del profilo in atto della persona a cui si riferiscono⁸.

FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in questo Volume, *retro*. Per un inquadramento più a cavallo tra diritto e società sia consentito anche rinviare a F. PIZZETTI, *Il prisma del diritto all'oblio*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, Giappichelli, Torino, 2013.

⁷ Parlano di un «più pragmatico *right not to be found*» in luogo del «*right to be forgotten*» A. PALMIERI - R. PARDOLESI in *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Nuovi quaderni del Foro italiano*, quaderno n. 1, 2014. Su questa specifica accezione del diritto all'oblio si è inoltre espresso l'International Working Group on Data Protection in Telecommunications (IWGDPT) nel documento *Recommendations on the Publication of Personal Data on the Web, Website Contents Indexing and the Protection of Privacy* (Praga 15-16 April 2013).

⁸ Si noti, a conferma di ciò che nel comunicato stampa della Corte di giustizia n. 70/14 del 13 maggio, relativo appunto ad illustrare il contenuto della decisione che qui si commenta, non si parla mai di diritto all'oblio o di *right to be forgotten* ma solo della responsabilità del gestore del motore di ricerca per i dati personali resi accessibili in quanto estratti da altri siti sorgente e del diritto dell'interessato a ottenerne la rimozione. Cfr. comunicato stampa della Corte di giustizia n. 70/14 del 13 maggio 2014, titolo e sintesi di sottotitolo. Coglie immediatamente, già il 13 maggio 2014, questo aspetto della questione L. MONTUORI, in *Diritto, mercato, tecnologie*, 13 maggio 2014.

3. I singoli criteri interpretativi affrontati nella decisione

Tornando al contenuto e all'impostazione argomentativa seguita dalla sentenza della Corte, va detto subito che la domanda pregiudiziale riguarda essenzialmente quesiti interpretativi relativi a una serie di disposizioni contenute nella Direttiva e nella Carta dei diritti dell'Unione Europea. Questi quesiti però sono posti unicamente al fine di valutare la legittimità della domanda di rimozione degli indici in possesso dei motori di ricerca relativi a dati personali dei richiedenti. Dunque al centro dei quesiti interpretativi sta sempre l'esistenza o meno di un diritto alla deindicizzazione⁹, che più pianamente, e con linguaggio meno cibernetico, potremmo definire diritto alla cancellazione dei dati, poggiate in questo caso, sugli art. 12, lettera *b*) e 14, primo comma lettera *a*) della direttiva¹⁰.

Il primo (art. 12, lettera *b*), notissimo, riguarda, tra l'altro, il diritto alla cancellazione o al congelamento dei dati il cui trattamento non è conforme alle disposizioni della Direttiva.

Il secondo (art. 14 primo comma, lettera *a*), non meno noto, stabilisce che l'interessato ha il diritto di opporsi in qualunque momento al trattamento di dati che lo riguardino, sempre che ricorrano ovviamente le condizioni previste dalla norma, e cioè: che vi siano motivi preminenti e legittimi derivanti dalla sua posizione personale; non vi sia disposizione contraria nella legislazione nazionale; ricorrano almeno i casi di cui all'art. 7, lettere *e*) ed *f*), relativi al trattamento di dati per l'esecuzione di un compito di interesse pubblico ovvero sia necessario ai fini del perseguimento dell'interesse legittimo del responsabile del trattamento o dei terzi cui vengono comunicati i dati, a condizione però che non prevalgano l'interesse, o i diritti, o le libertà fondamentali della persona interessata, tutelati dall'art. 1, paragrafo 1 della Direttiva.

⁹ Mettono bene in luce questo specifico aspetto, al quale dedicano ampia ed esauriente attenzione, S. SICA - V. D'ANTONIO, *La procedura di de-indicizzazione*, in questo Volume, *retro*. Sui temi legati alla deindicizzazione e in genere agli aspetti tecnologici applicati alla conoscibilità, alla conservazione, alla ricerca e alla cancellazione dei dati sulla rete cfr. G. D'ACQUISTO, *Diritto all'oblio: tra tecnologia e diritto*, in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, op. cit.

¹⁰ In questo senso anche il c.d. *right not to be found easily* è un puro aspetto descrittivo dell'effetto che ha la cancellazione (deindicizzazione) sul motore di ricerca ma non è una figura giuridica a sé stante, della quale peraltro non si trova traccia nella direttiva e nemmeno nel Regolamento proposto dalla Commissione e ancora in discussione. A differenza invece del *right to be forgotten*, ora diventato, nel testo del nuovo Regolamento approvato dal Parlamento europeo *right to erasure* che tuttavia non è, neppure esso, il diritto all'oblio come comunemente lo si intende.

Ovviamente per poter affermare, sulla base di queste disposizioni, la legittimità della richiesta di deindicizzazione la Corte deve prima affrontare e superare una serie di passaggi e risolvere le diverse questioni poste nella articolata domanda di pronuncia pregiudiziale.

3.1. La qualificazione della attività svolta dai motori di ricerca

Innanzitutto la Corte stabilisce che l'attività di un motore di ricerca «consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet»¹¹, deve essere qualificata trattamento di dati personali ai sensi dell'art. 2 lettera *b)* e *d)* della Direttiva. La Corte usa a questo fine argomenti che già erano presenti in vari provvedimenti di Garanti nazionali ed europei: in particolare, e in modo esteso, nella *opinion* del WP29 n. 148 adottata il aprile 2008 e dedicata proprio ad esaminare «gli aspetti della protezione dei dati connessi ai motori di ricerca»¹².

Una opinione, quest'ultima, estremamente raffinata, che avvalendosi anche del precedente parere sul concetto di dato personale adottato l'anno prima con la *opinion* WP29 n. 136, riconosce innanzitutto che l'attività dei motori di ricerca implica il trattamento di dati personali, per prendere poi in esame tutti i diversi tipi di trattamento che essi fanno relativamente ai dati raccolti sulla rete.

3.2. Il gestore del motore di ricerca come titolare dei trattamenti

Il secondo quesito al quale la Corte deve rispondere è se il motore di ricerca sia responsabile anche di quel particolare tipo di trattamento dati che consiste nel mettere a disposizione degli utenti di Internet, secondo un dato ordine di preferenza, i dati personali raccolti in rete.

La Corte senza grandi esitazioni dice di sì. Sottolinea infatti che «il gestore di un motore di ricerca 'raccolge' dati personali che 'estrae', 'registra' e successivamente 'organizza' nell'ambito dei suoi programmi di indicizzazione, 'conserva' nei suoi server e, eventualmente, 'comunica' e 'mette a disposizione' dei propri utenti sotto forma di elenchi dei risultati delle

¹¹ Così la Corte definisce l'oggetto della questione nella parte dispositiva punto 1).

¹² Così infatti il titolo della *opinion* WP n. 148.

loro ricerche»¹³. Pertanto, continua la Corte, «è il gestore del motore di ricerca che determina le finalità e gli strumenti di tale attività e dunque del trattamento dei dati personali che egli stesso effettua nell'ambito dell'attività medesima» «è di conseguenza lui che a dover essere considerato titolare di tale trattamento a norma dell'art. 2 lettera *d*)» della direttiva¹⁴.

Su questo punto esiste una differenza netta fra questa decisione e il parere n. 148 del WP29.

In quel parere, infatti, il WP29 aveva scelto di analizzare «partitamente e separatamente» i molti diversi tipi di trattamento dei dati personali che possono essere oggetto dell'attività dei gestori dei motori di ricerca, stabilendo poi, per la quasi generalità dei diversi tipi di trattamento individuati, prescrizioni specifiche, ora in termini di divieto, ora in termini di obbligo di informativa, ora in termini di obbligo di consenso¹⁵.

Aveva però esplicitamente, e per la verità in modo piuttosto sbrigativo, escluso che il gestore di ricerca fosse responsabile proprio del trattamento consistente nell'indicizzazione e messa a disposizione degli utenti dei dati personali riferiti a singoli interessati raccolti sulla rete.

Aveva detto infatti il WP29 al punto 4.2.2 della *opinion* che «il principio di responsabilità comporta che, nella misura in cui interviene esclusivamente come intermediario, il provider di motori di ricerca non deve essere considerato il responsabile principale del trattamento con riguardo

¹³ Cfr. punto 28 della parte motiva della decisione della Corte.

¹⁴ Cfr. punto 33 della parte motiva della decisione.

¹⁵ Sulla scia di alcune indicazioni e raccomandazioni contenute nella *opinion* WP29 n. 148 sono stati successivamente adottati molti provvedimenti da parte delle Autorità nazionali rispetto ai trattamenti specifici oggetto di quella *opinion*. Inoltre, sempre muovendo da quanto in essa affermato, si sono svolte anche attività di indagine coordinate tra le Autorità in ordine ai trattamenti effettivamente svolti. Tra questi provvedimenti possiamo ricordare, in particolare, il recente provvedimento della Autorità garante italiana per la protezione dei dati personali n. 353 del 2014 a contenuto prescrittivo nei confronti di Google inc. «sulla conformità al Codice dei trattamenti di dati personali effettuati ai sensi della nuova *privacy policy*» adottato il 10 luglio 2014. Su tematica analoga anche il provvedimento sanzionatorio adottato dalla CNIL il 3 gennaio 2014 col quale la Autorità francese, anche tenendo conto dei risultati emersi nell'ambito dell'attività di indagine coordinata condotta dalle Autorità europee, e ritenendo che sulla base dei risultati raggiunti vi fossero significative violazioni della legge di protezione dati francesi conseguenti alla *privacy policy* adottata, ha comminato una sanzione di 150.000 euro alla società Google inc. Analogo provvedimento, anch'esso collegato alla medesima indagine conoscitiva, è stato adottato dalla Autorità spagnola. Il Direttore della AEDP J.L. Rodriguez Alvarez, con provvedimento del 19 dicembre 2013, ha comminato a Google inc. una sanzione di 300.000 euro per ciascuna di una serie di violazioni della legge spagnola di protezione dati (LOPD) specificamente individuate nel provvedimento stesso.

al trattamento dei dati personali... resi accessibili agli utenti della rete».

Secondo il WP29 il controllo di tipo formale, giuridico e pratico che i gestori dei motori di ricerca esercitano sui dati personali si limita di solito alla possibilità di cancellarli dal server. Essi dunque possono essere al massimo considerati responsabili per quanto riguarda la cancellazione ma a stabilire se sussista o no questo obbligo, conclude il WP29, «possono essere le norme generali sulla responsabilità civile vigenti in un determinato Stato membro».

In sostanza, nella *opinion* n. 148 il WP29 non solo non sviluppò gli approfonditi (e convincenti) ragionamenti fatti oggi dalla Corte di giustizia, ma seguì una linea argomentativa assai parziale, chiaramente finalizzata a non voler ricondurre sotto la competenza della Direttiva, e dunque delle Autorità garanti, l'attività di indicizzazione e messa a disposizione dei dati personali raccolti in rete dai motori di ricerca.

Il WP29 volutamente vide infatti essenzialmente l'aspetto, che nemmeno la Corte nega, dei motori di ricerca come *media* della società dell'informazione e quindi considerò l'attività di indicizzazione soltanto come messa a disposizione degli utenti di informazioni, nel quadro esclusivo dell'attività di informazione (v. WP29, *opinion* n. 148, punto 2).

Non a caso al fine di rafforzare la successiva esclusione di questo tipo di attività dei motori di ricerca dalla Direttiva e, soprattutto, della competenza delle Autorità garanti, l'*opinion* n. 148 del 2008 cita soltanto l'art. 11 della Carta dei diritti dell'Unione, nella parte in cui stabilisce che l'accesso alle informazioni deve avvenire senza controllo da parte delle Autorità pubbliche.

La Corte cita invece in senso opposto l'art. 7 e l'art. 8 della Carta, nella parte in cui tutelano la dignità delle persone e la protezione dei dati personali. Afferma infatti la Corte che «i diritti tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet», pur se possono esserci situazioni in cui «il giusto equilibrio può dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare a seconda del ruolo che la persona riveste nella vita pubblica» (cfr. punto 81 della parte motiva della sentenza)¹⁶.

¹⁶ Critica questo aspetto della decisione della Corte di giustizia O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo. Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in questo Volume, *retro*. Al titolo così suggestivo si potrebbe però obiettare che, al contrario, a suo tempo il WP29 nell'*opinion* n. 148 del 2008 ha forse preso troppo sul serio l'art. 11 della Carta, e lo dice chi a suo

Questo è dunque il punto in cui la Corte di giustizia più si differenzia dal parere n. 148 del WP29.

Non a caso è anche il punto in cui la sentenza si differenzia di più dal parere dell'Avvocato generale Jääskinen e dalle previsioni fatte da molti autori sul probabile esito della causa¹⁷.

Previsioni che peraltro, a mente più fredda, forse erano un poco troppo sbrigative, tenendo conto che dopo il 2008 già molte Autorità nazionali avevano dedicato particolare attenzione agli operatori su Internet e in qualche caso, anche prima della opinion n. 148, già si era detto con chiarezza che i motori di ricerca e i trattamenti legati all'indicizzazione dei dati modificavano profondamente il significato dei dati stessi come messi in rete dai siti fonti, e dunque costituivano trattamenti a sé stanti, di cui era responsabile il gestore del motore di ricerca¹⁸.

Certo non si era ancora mai giunti a sanzionare la diretta responsabilità di Google o di altri motori di ricerca ma, almeno nel caso del Garante italiano, non tanto perché i trattamenti non fossero riconducibili ai motori di ricerca e alla loro responsabilità, quanto piuttosto per la convinzione che nell'ambito della Direttiva fosse difficile radicare la competenza dell'Autorità nazionale rispetto a trattamenti fatti da server collocati in territori estranei allo Stato¹⁹.

In ogni caso il 'salto' compiuto dalla decisione della Corte di giustizia è su questo punto fortemente innovativo e costituisce un cambiamento profondo che colloca ormai a pieno titolo le attività dei motori di ricerca all'intero tematica di applicazione della Direttiva.

tempo, nella qualità di Presidente dell'Autorità italiana approvò l'*opinion* insieme agli altri colleghi.

¹⁷ Alle conclusioni dell'Avvocato generale Jääskinen., per dimostrare che la Corte ha voluto dare eccessiva tutela al diritto all'oblio (che come abbiamo visto non è preso affatto in considerazione dalla Corte), danno molta attenzione M. BASSINI e O. POLLICINO in «*Bowling for Columbine. La Corte di giustizia sul caso Google Spain: l'oblio (quasi) prima di tutto?*», in *Diritto24*, 13 maggio 2014. Un commento forse troppo immediatamente a ridosso della sentenza della Corte, che riletto oggi appare forse un pochino troppo critico della decisione.

¹⁸ In questo senso si era pronunciato, fin dal 2006 il Garante italiano, nel primo provvedimento in assoluto adottato nell'Unione Europea in cui si è affermato che l'attività di indicizzazione svolta dai motori di ricerca costituisce trattamento dati e che il gestore ne è responsabile. Cfr. *doc. web n. 1242501 del 18 gennaio 2006*, ora reperibile anche in M. PAISSAN, *Privacy e giornalismo*, seconda edizione aggiornata, edizioni del Garante, Roma, 2008, p. 330.

¹⁹ Si veda in questo senso la chiarissima lettera inviata da chi scrive, quale allora Presidente del Garante italiano, a Google Inc. in data 22 marzo 2006, *doc. web n. 1339146*, ora in M. PAISSAN, *Privacy e giornalismo op. cit.* p. 333.

Prima di concludere su questo punto vale la pena osservare che anche su questo aspetto così innovativo, e di fatto così diversamente impostato rispetto al WP29 nella sua *opinion* n. 148, i Garanti europei hanno dimostrato convinta adesione (cfr. Comunicato stampa WP29 del 23 Maggio 2014).

3.3. Il principio di stabilimento e la sua applicabilità ai motori di ricerca

Stabilito che l'attività svolta dal gestore rispetto alla raccolta dei dati personali in rete e alla loro indicizzazione rientra sotto la Direttiva e fa assumere al gestore la qualifica di titolare del relativo trattamento, la Corte ha dovuto affrontare un altro aspetto, anch'esso posto nella domanda di decisione pregiudiziale rivolta dalla *Audiencia Nacional*, e cioè se la Direttiva UE fosse applicabile anche ai trattamenti posti in essere da gestori i cui server fossero collocati in territori diversi da quelli degli Stati membri dell'Unione.

La Corte ha dovuto pertanto confrontarsi col principio di stabilimento, aspetto essenziale, come è ben noto, per radicare la applicabilità della normativa europea e soprattutto la competenza degli Stati membri ai sensi dell'art. 4 paragrafo 1 della Direttiva.

Anche qui la Corte ha assunto una posizione molto innovativa. Ha stabilito infatti che il requisito previsto dall'art. 4 paragrafo 1 lettera *a*), riferito proprio al principio di stabilimento, è soddisfatto «qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinate alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca e la cui attività si dirige agli abitanti di detto Stato» (cfr. punto 2 della parte dispositiva).

Ha legato cioè il concetto di stabilimento non necessariamente al luogo dove il trattamento è concretamente effettuato ma a quello dove il trattamento esplica i suoi effetti (luogo di destinazione del servizio) e all'esistenza nel medesimo territorio di uno stabilimento nel «contesto delle attività» del quale il trattamento è effettuato. È questo uno dei punti di maggiore interesse della decisione²⁰. Non sono mancati in questi anni

²⁰ Colgono bene questo aspetto G. BUSIA e L. MONTUORI, *Diritto, mercato ecc. opp. locc. cit.* Va sottolineato, a margine, che il nuovo principio stabilito dalla Corte di giustizia colloca ora in una luce del tutto nuova il tema della c.d. *web tax*, posto inopportunitamente da ultimo dalla Commissione bilancio della Camera, e dal suo Presidente F. Boccia fortemente difesa, solo due mesi prima di questa decisione e successivamente cancellata dal Governo Renzi nel primo Consiglio dei ministri dopo la sua entrata in carica. Una delle

provvedimenti dei Garanti nei confronti dei provider di diverse categorie dei cosiddetti servizi della società dell'informazione, ma sempre si è radicata la legittimità a intervenire sul fatto che l'attività connessa al trattamento avvenisse sul territorio nazionale, fosse anche solo per la parte finale del trattamento stesso²¹.

In questo caso, invece, anticipando in parte il contenuto del nuovo Regolamento europeo, si afferma in modo esplicito che anche semplicemente la attività di raccolta pubblicitaria o altra attività commerciale, ove sia strettamente connessa ai trattamenti dati ed anzi ne costituisca una delle finalità principali, radica il principio di stabilimento all'interno dello Stato in cui questo avviene. Anche questa innovazione è stata accolta con favore dai Garanti europei, che hanno segnalato la loro approvazione già nel comunicato stampa del 23 maggio, precedentemente segnalato.

3.4. La legittimità della richiesta di deindicizzazione e il combinato disposto art. 14 primo comma lettera a) e art. 7 lettere e) e f) della Direttiva

Infine la Corte ha dovuto affrontare un'ultima questione, non posta esplicitamente dalla *Audiencia Nacional* ma implicita nel ragionamento stesso svolto dalla Corte medesima. Come si è detto la Corte radica il diritto a ottenere la deindicizzazione dei dati personali negli art. 12 lettera b) e 14, primo comma lettera a), e cioè sulle norme che consentono all'interessato di esercitare, tra l'altro, il diritto alla cancellazione del dato quando ricorrono le circostanze indicate nelle due norme.

A tal fine, avendo presente quanto contenuto nell'art. 14 primo comma lettera a), occorre dimostrare che il trattamento dei dati di cui si chiede la cancellazione (in questo caso la deindicizzazione) rientri almeno

obiezioni che anche chi scrive formulò a quella presa di posizione della Commissione bilancio della Camera riguardò infatti proprio l'aspetto della legittimità di un prelievo disposto nei confronti di società di servizi (Google Italia e altre società dei social operanti in Italia) che allora non potevano essere considerati responsabili per i trattamenti effettuati dai server delle rispettive 'Case madri' in territorio non italiano. Ora, alla luce di questa decisione, il quadro appare del tutto modificato. Cfr. per una ricostruzione esauriente della vicenda, che occupò molto a quel tempo i giornali specializzati e non, la ricostruzione fatta dal quotidiano online *Il Post*, 16 dicembre 2013, le obiezioni espresse dalla Commissione Europea riportate da *Il Sole 24 Ore* nel numero del 19 dicembre e il comunicato stampa del Governo Renzi del 28 febbraio 2014 il cui contenuto è riportato da Rep.it in pari data.

²¹ Cfr. in questo senso, *ex pluribus*, i provvedimenti del Garante italiano del 7 aprile 2011 e del 6 ottobre 2011 in materia comunicazioni promozionali automatizzate, rispettivamente documento web n. 1810207 e documento web n. 1851750.

in uno dei casi previsti dall'art. 7, lettere *e*) e *f*). Casi, questi, nei quali la cancellazione (deindicizzazione) può essere chiesta anche solo per «motivi preminenti e legittimi derivanti dalla posizione particolare della persona interessata».

Diventa di conseguenza essenziale per la Corte individuare quali siano le finalità del trattamento di deindicizzazione dei dati personali sui motori di ricerca, se non altro per verificare se, in ragione di tali finalità, il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 7, lettera *c*), ovvero sia necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure dei terzi a cui vengono comunicati i dati.

Sulla base dell'analisi svolta e ampiamente approfondita nella parte motiva della decisione (in particolare nei punti da 34 a 38) la Corte sottolinea che le finalità perseguite dal gestore del motore di ricerca sono almeno due.

La prima, strettamente legata al *business* del gestore per il quale i dati sono un valore in virtù degli accessi che determinano, e gli accessi sono un valore economico grazie alla raccolta pubblicitaria che costituisce la ragione stessa dell'attività economica del gestore.

Raccolta pubblicitaria che, a sua volta, costituisce lo scopo principale delle consociate nazionali operanti nel territorio degli Stati membri che, e per questo, sono strettamente connesse all'attività del gestore (cfr. in particolare i punti da 55 a 58 della decisione).

La seconda finalità è legata invece al riconoscimento che l'attività del gestore è anche strettamente connessa all'interesse legittimo degli utenti di Internet ad avere accesso all'informazione così come fornita dal motore di ricerca. Una informazione che, per comune riconoscimento, non è la medesima postata sui siti fonti perché, in virtù appunto del trattamento, assume una sua originalità e una sua valenza specifica.

Questa doppia finalità, quella legata all'attività economica propria del gestore e al trattamento dati come oggetto di un'attività che li trasforma in valore economico, e quella legata al fornire agli utenti della rete una informazione autonoma e diversa da quella contenuta nei siti fonte è ampiamente sottolineata in molti punti della parte motiva ed è considerata dalla Corte come il perno intorno al quale ruota la decisione. Non a caso la Corte, nel far riferimento all'art. 14 primo paragrafo lettera *a*), richiama anche l'art 7 lettera *f*) della Direttiva che ricomprende sia il caso di trattamento dati necessario per perseguire l'interesse legittimo del titolare del trattamento, che quello finalizzato all'interesse dei terzi cui

vengono comunicati i dati (cfr. punto 86 della parte motiva). Non vi è dubbio che in questa decisione il diritto alla cancellazione (*rectius*: deindicizzazione) fondato sull'art. 14 lettera *a*), e dunque sul prevalere di motivi legittimi e preminenti dell'interessato rispetto alle finalità del trattamento, ricomprende non solo la parte relativa alla finalità *business* del gestore, ma anche quella di servizio di informazione per gli utenti della rete, e dunque riguarda i motori di ricerca anche dal punto di vista del loro essere *media* della società dell'informazione. Aspetto, quest'ultimo, che la Corte non ignora né sottovaluta ma che, al contrario del WP29 nella *opinion* n. 148, non considera né l'unico né il prevalente.

3.5. Il punto essenziale: il diritto dell'interessato alla deindicizzazione prevale di massima sull'interesse del gestore e su quello degli utenti

Se questa ricostruzione è corretta, è chiaro dunque che in questa decisione il diritto alla cancellazione (deindicizzazione) di dati personali chiesto dall'interessato per motivi preminenti e legittimi prevale non solo sull'interesse economico del trattamento da parte del titolare ma anche su quello a essere informati degli utenti.

Cosa questa che troppo spesso in molti commenti è sottovalutata o non adeguatamente colta.

Può piacere o no, può essere condivisibile o no, ma questo è l'aspetto più importante, nuovo e originale della decisione.

3.6. Il diritto degli utenti all'informazione come limite al diritto dell'interessato, condizionato all'esistenza di situazioni specifiche

Resta certamente vero che la Corte introduce comunque un limite al prevalere del diritto dell'interessato che è strettamente legato al servizio informativo reso dal motore di ricerca. Il riferimento è a quella parte della decisione, contenuta nel punto 97, in cui la Corte individua come limite al diritto di cui all'art. 14 primo periodo, letto alla luce degli art. 7 e 8 della Carta, proprio l'interesse degli utenti della rete a conoscere quando questo sia qualificato dalla particolare natura dei dati o, più precisamente, delle caratteristiche proprie dell'interessato stesso, come avviene quando questo ricopra un ruolo nella vita pubblica.

Ovviamente, dato il tenore quasi di nota a margine proprio di quanto affermato a questo proposito nel punto 97, si può ritenere che il riferimen-

to all'eventuale ruolo di persona pubblica dell'interessato si configuri quasi come un esempio o una sorta di richiamo di stile per dire che vi sono casi in cui, o in ragione del dato o in ragione della persona alla quale il dato si riferisce, l'interesse degli utenti della rete a conoscere può prevalere sul preminente motivo legittimo dell'interessato a ottenere la cancellazione (la deindicizzazione del dato). In ogni caso però quanto detto nel punto 97, anche se interpretato in modo estensivo, si configura sempre come un limite a un diritto alla cancellazione dei dati che, ove ricorrano le condizioni indicate dalla Corte, prevale sia sulla finalità di *businnes* che su quella di informazione agli utenti.

4. *Il 'nocciolo duro' della questione*

Siamo dunque di fronte a una decisione che rovescia molte letture e molte impostazioni consolidate del rapporto tra tutela del diritto dell'interessato alla cancellazione del dato e tutela dell'interesse pubblico a conoscere.

Una decisione che rifiuta a priori di essere costretta nei tradizionali binari del 'diritto all'oblio' *versus* «diritto ad informare e ad essere informati» nel quadro della libertà di stampa e soprattutto della libertà di manifestazione del pensiero. Prima di trarre conclusioni troppo affrettate, però, occorre ribadire un aspetto già sottolineato più volte e notissimo a tutti i commentatori, ma troppo spesso sottovalutato. Peraltro la decisione si limita a prendere in esame la domanda di pronuncia pregiudiziale, e quindi si limita a giudicare del diritto a ottenere la deindicizzazione dei dati personali sui motori di ricerca.

Per questo non si tratta di una decisione in materia di diritto all'oblio. Essa infatti non garantisce affatto che la informazione di cui si chiede la cancellazione sia espunta dalla rete, ma solo dal motore di ricerca²².

²² Per questo non vengono qui in ballo i temi delicatissimi del rapporto tra diritto all'oblio e diritto alla memoria, né quelli relativi alla tutela del fatto storico *versus* il valore del suo aggiornamento, che sono invece, al di là dei temi legati alla libertà di stampa e di manifestazione del pensiero, stati bene al centro del dibattito sulla notissima decisione della Corte di Cassazione civile italiana n. 5525 del 2012. Una decisione che ha suscitato un dibattito approfondito proprio sui temi della memoria e dei modi e dei limiti di modifica del fatto storico finalizzati a tener conto di quanto successivamente avvenuto. Si veda su questo la interessante e divergente posizione di A. MANTELERO, *Il diritto all'oblio dalla carta stampata a internet*, e L. FEROLA, *Riservatezza, oblio, contestualizzazione: come è mutata l'identità personale nell'era di Internet*, entrambi in F. PIZZETTI (a cura di), *Il*

Per questo non viene messa in gioco la libertà di stampa e di manifestazione del pensiero. Essa infatti si occupa dell'interesse degli utenti a conoscere i dati accessibili in rete solo in virtù del fatto, che è alla base stessa del riconoscere i motori di ricerca come responsabili del trattamento, che una lista organica di notizie e dati offre una informazione ulteriore e diversa rispetto ai siti fonte. Il contrario vale per la libertà di manifestazione del pensiero o di stampa che sulla rete si esercita normalmente attraverso i siti fonte.

Per questo non è una decisione che si pone il problema del corretto bilanciamento tra diritto alla cancellazione e diritto all'accesso al dato in nome della trasparenza e del controllo democratico delle attività alle quali i dati si riferiscono. Sia la trasparenza, qualunque cosa questa significhi, che la accessibilità ai dati ai fini di controllo democratico sono garantite innanzitutto dall'accesso ai siti fonte che prescindono dai motori di ricerca.

Per questo non è una decisione che si pone il problema di trovare il corretto bilanciamento tra diritto all'oblio e diritto alla memoria. La memoria intesa come conservazione dei dati in rete non è messa in pericolo dalla deindicizzazione dei dati personali sul motore di ricerca ma caso mai dalla loro cancellazione sui siti fonte.

Cancellazione che però non costituisce in alcun modo oggetto di questa decisione.

Sarebbe tuttavia superficiale limitarsi a sottolineare soltanto che oggetto della decisione è il diritto o la legittimità della richiesta di deindicizzazione.

Il contenuto della sentenza va molto oltre.

La base di tutto è il riconoscimento che il motore di ricerca, indicizzando i dati accessibili in rete in base a modalità decise autonomamente dal gestore, muta anche il contenuto comunicativo e informativo dei dati che tratta, rendendoli tutti parte di una informazione attuale che, in virtù della loro aggregazione e della loro indicizzazione, è comunque diversa da quella che ciascuno di essi separatamente, e in quanto accessibile consul-

caso del diritto all'oblio, Giappichelli, Torino, 2012. In quella stessa raccolta, proprio sul tema dell'oblio e della memoria si veda anche l'approfondimento di M. DURANTE e U. PAGALLO, *Diritto, memoria e oblio* e le considerazioni di T. E. FROSINI, *Il diritto all'oblio e la libertà informatica*. Sul medesimo tema e in particolare sulla citata decisione della Corte di Cassazione la letteratura italiana è per altro ormai amplissima. Una rassegna importante di tale letteratura è riportata in A. PALMIERI - R. PARDOLESI, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, op. loc. cit., nota 14.

tando direttamente i siti fonte, fornisce²³.

Qui sta il punto essenziale.

Il motore di ricerca è un *media* della società dell'informazione ma dà informazioni per loro natura diverse e potenzialmente assai più invasive di quelle accessibili direttamente in rete. Questo aspetto è considerato giustamente dalla decisione non solo come un arricchimento ma anche come un potenziale o attuale pericolo per la dignità delle persone a cui le informazioni si riferiscono.

Questo per almeno due ordini di motivi: il primo, che proprio in virtù del motore di ricerca, le informazioni indicizzate mutano natura, se non altro perché consentono una profilazione che i siti fonte non consentono; il secondo, che le informazioni indicizzate e rese accessibili dal motore di ricerca sono sottoposte a una continua attualizzazione mentre, al contrario, i siti fonte mantengono invece la loro corretta conoscibilità storica o comunque temporale.

È questa la ragione del perché questa decisione sposta il punto di equilibrio della bilancia tutto a favore della protezione dei dati personali e dunque dell'accoglibilità delle richieste, individuando come unico limite la sussistenza di specifiche, e per il vero non così compiutamente individuate, caratteristiche dei dati o degli interessati ai quali i dati si riferiscono, con particolare riguardo al carattere pubblico dell'interessato stesso.

Insomma, questa è una decisione che, sapendo che il motore di ricerca è un *media* che fornisce una informazione diversa, più strutturata e comunque permanentemente attualizzata rispetto a quella accessibile sui siti fonte, tutela e protegge più l'interessato dal pericolo che sia lesa la sua dignità e profilata indebitamente la sua personalità che non l'interesse degli utenti a acquisire elementi informativi, che comunque non sono più quelli originari. Può piacere o no, si può condividere o no, ma questo è il nocciolo duro e il significato profondo di questa decisione.

5. A proposito di alcune censure espresse dalla dottrina

Se questa ricostruzione è corretta, perde molto di interesse e di fondamento anche la obiezione che la decisione individua nel gestore il desti-

²³ Mostra di cogliere bene questo aspetto e di interrogarsi a fondo proprio su questo punto A. MANTELERO, *Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy*, in questo Volume, *retro*.

natario primo della richiesta e nelle Autorità solo un secondo momento di appello contro il diniego all'accoglimento della richiesta da parte del gestore. Critica che di solito muove dall'osservazione che ciò significa attribuire al gestore un compito che ha una forte valenza pubblicistica connessa al carattere informativo dei motori di ricerca²⁴. Allo stesso modo perde molto di importanza l'osservazione che la decisione non prevede che siano informati della richiesta i soggetti che hanno postato in rete le informazioni di cui si chiede la indicizzazione, nemmeno se questi sono a loro volta soggetti della società dell'informazione, o direttamente dei *media* ai quali si riconduce istituzionalmente sia la libertà di stampa che di manifestazione del pensiero²⁵.

È evidente che la Corte ritiene che la informazione offerta dai motori di ricerca, proprio perché 'diversa' e 'altra' rispetto a quella offerta dai siti fonte, non riguardi, almeno in linea di massima, chi ha postato in rete i dati che successivamente il motore ha raccolto e indicizzato. Allo stesso modo si può comprendere che la Corte non si sia fatta alcuno scrupolo di affidare al gestore, e solo al gestore, la decisione se accogliere o meno la richiesta. Infatti la informazione offerta dal gestore non è quella originale postata sulla rete e dunque la deindicizzazione non mette affatto in pericolo il diritto a conoscere, né il diritto a conservare, né tanto meno la libertà di stampa o di manifestazione del pensiero.

La Corte, non ritiene dunque che vi sia motivo per riservare solo alle Autorità la decisione sulla richiesta, derogando così a un sistema che invece vede nel titolare del trattamento il primo e naturale destinatario delle richieste di cancellazione del dato. Infine, come si è già detto, non vi è alcuna ragione, secondo la Corte, per costruire una sorta di diritto di terzi ad essere informati della richiesta, siano anche i titolari del trattamento originario in virtù del quale il dato è stato prodotto e postato in rete. Nella logica di questa decisione il carattere informativo preso in considerazione

²⁴ Quello che più ha sottolineato questo aspetto fin dai primi commenti alla decisione è stato O. Pollicino. Cfr. O. POLLICINO e M. BASSINI, *Bowling for Columbine*, op. loc. cit., e ID., *Il diritto all'oblio preso sul serio*, in *Confronti costituzionali*, 16 maggio 2014. In senso diverso, invece, fin dai primi commenti, l'opinione di chi scrive. Cfr. F. PIZZETTI, *La decisione della Corte di Giustizia sul caso Google Spain: più problemi che soluzioni*, in *Federalismi*, 10 giugno 2014.

²⁵ Quasi tutti i commentatori, vedendo in questa decisione essenzialmente il limite all'accessibilità all'informazione in rete, hanno fatto questa osservazione. Cfr. fra i tanti, in particolare, G.M. RICCIO, *Diritto all'oblio e responsabilità del motore di ricerca*, in questo Volume, *retro*. e S. SICA e V. D'ANTONIO, *La procedura di de-indicizzazione*, *ibidem*. Questo aspetto ha inoltre avuto anche una particolare enfaticizzazione nel dibattito internazionale.

è solo quello legato alla attività svolta dal motore di ricerca, indipendentemente dalle finalità per le quali le informazioni trattate sono state postate nei siti sorgente o messe comunque in rete²⁶.

In sostanza, e questa è la tesi che qui si vuole sostenere, la decisione non appare così censurabile come molti commentatori hanno ritenuto. Tutto ruota infatti intorno alla distinzione tra informazione postata in rete nei siti fonte e informazione di diversa 'natura', e anche di diversa 'pericolosità' per la dignità e i diritti fondamentali degli interessati, che i motori di ricerca rendono accessibili agli utenti.

Questo peraltro spiega bene anche perché la Corte sia molto parca nell'indicare quali siano le circostanze che il gestore deve tenere presenti nel valutare la richiesta di deindicizzazione. Mancano infatti nella sentenza paletti precisi che limitino l'accoglibilità della richiesta, e tanto meno sono ripetuti i principi tradizionali che caratterizzano secondo la dottrina il diritto all'oblio, quali l'attualità della notizia o il persistente interesse pubblico a conoscerla.

Il fatto è che la Corte non pensa mai all'informazione originaria (o per così dire allo stato puro) postata in rete sui siti fonte, ma si occupa sempre e soltanto dell'informazione come intesa nell'ambito dei motori di ricerca e della 'manipolazione' che essi fanno dei dati personali raccolti in rete. Dunque, non deve stupire poi troppo che il motore di ricerca possa essere spinto ad accogliere con una certa larghezza le richieste di deindicizzazione, e ciò non solo per evitare banalmente eventuali richieste di danni qualora poi le Autorità dessero ragione ai richiedenti, ma anche perché è nella logica della decisione della Corte favorire più l'accoglimento che non il rigetto delle richieste.

²⁶ È interessante tuttavia osservare come, per le prime informazioni che vengono raccolte sulle modalità realizzative del dispositivo delle sentenze, Google sembra intenzionata a notificare ai siti sorgente l'avvenuta de-indicizzazione dei link riferibili agli interessati che si siano avvalsi del *form on-line* appositamente predisposto dalla società per accogliere le richieste di cancellazione, invertendo in un certo qual modo l'ordine logico dell'art. 17, comma 2, del nuovo Regolamento Europeo in materia di protezione dei dati, così come approvato in prima lettura dal Parlamento europeo nel marzo 2014. Mentre infatti nella formulazione del legislatore europeo è il gestore del sito sorgente a dover 'inseguire' il dato della cui diffusione si è reso responsabile (arrivando a porre in capo a questo soggetto l'onere di richiederne la cancellazione dai siti 'terzi'), più pragmaticamente, e forse più correttamente vista la capacità di diffusione del dato operata dal motore di ricerca, Google stessa sta operando in modo da rendere il sito sorgente consapevole della avvenuta deindicizzazione. Questo anche per consentire a quest'ultimo una eventuale (e più efficace) deindicizzazione *ex-ante*, con gli strumenti tecnologici di cui dispone. Ma sui limiti 'interpretativi' del Regolamento rispetto ai fenomeni che avvengono oggi su Internet, dai motori di ricerca alle social network, si tornerà più avanti.

6. La eccessiva genericità dei criteri indicati al punto 97 della sentenza relativamente al limite dell'accogliibilità della richiesta. I condizionamenti posti dalla direttiva e i nodi non sciolti dal nuovo regolamento. Verso un 'procuratore ai dati'

Ma.. vi è.. un ma: ed è che la Corte stessa al punto 97 individua un limite all'accoglimento della richiesta, riferito genericamente tanto alla natura dei dati che alle caratteristiche dell'interessato. Qui, proprio nel punto 97, vi è il principale aspetto di debolezza della decisione e in questo si possono radicare le principali ragioni di critica.

Nel momento stesso in cui, all'interno di un ragionamento tutto orientato a massimizzare il diritto alla cancellazione rispetto all'interesse del gestore e degli utenti della rete, la Corte pone un limite così rilevante, individuato nella eventualità che, o in ragione della natura dei dati, o in ragione delle caratteristiche dell'interessato, possa prevalere l'interesse degli utenti all'informazione, la Corte avrebbe avuto il dovere di precisarne assai di più il contenuto.

Non solo: proprio l'individuazione di questo limite, che è certo assai più potenzialmente ampliabile di quanto il punto 97 sbrigativamente indichi, giustifica in parte l'interrogativo di chi si chiede se sia corretto porre sulle spalle del gestore, in dialogo con l'interessato, ogni scelta sui criteri in concreto da adottare rispetto alle singole richieste.

Si sconta qui il limite intrinseco della protezione dei dati personali come concepita nella Direttiva, e quindi anche i limiti di una Direttiva adottata prima dello sviluppo commerciale di Internet e, soprattutto, molto prima del web 2.0.

Non vi è spazio, infatti, nella Direttiva per individuare una sorta di 'procuratore ai dati' che possa difendere, in contraddittorio col gestore e il richiedente, anche le ragioni degli utenti, né sembra ragionevole che solo rispetto ai motori di ricerca si debba e si possa imporre obbligatoriamente il ricorso immediato diretto alle Autorità garanti o al giudice.

Di fatto, e proprio su questo punto, la decisione mostra in controluce tutti i limiti della attuale Direttiva e la grande difficoltà, per non dire la impossibilità, di restringere dentro i suoi confini la protezione dei dati sulla rete, specie con riferimento ai nuovi trattamenti legati ai motori di ricerca e ai *social*.

Da questo punto di vista anche il nuovo Regolamento proposto dalla Commissione, e ormai da anni all'esame delle istituzioni dell'UE, non pare destinato a risolvere tutti i problemi, e certamente non quelli posti

da questa decisione.

Pur registrando che per fortuna nel testo approvato dal Parlamento europeo il titolo dell'art. 17 è stato modificato, rinunciando all'equivoco e sempre discutibile 'diritto all'oblio' per un più modesto ma ben più solido 'diritto alla cancellazione' dei dati personali, resta fermo che anche in questo testo, come in quello precedente, la tutela assicurata è certamente ampliata rispetto alla Direttiva ma si continua a non distinguere adeguatamente tra la natura propria dei dati personali postati in rete in quanto tali, su siti sorgente che li contengono e li trattano per finalità specifiche, dai dati che invece sono oggetto di indicizzazione da parte dei motori di ricerca o che sono diffusi secondo le modalità proprie dei *social*. Modalità, queste, che nella loro amplissima variabilità, spesso consentono, o comportano, automaticamente l'incrocio o la connessione dei dati di un sito con altri dati riferiti alla medesima persona postati in rete in altri siti e per altre finalità, ovvero anche l'incrocio con dati personali riferiti ad altre persone connessi nelle modalità più diverse con quelli del richiedente.

In questo senso anche la normativa del Regolamento europeo, pur attenta per quanto possibile a calare la tutela dei dati personali anche all'interno del diverso 'ambiente' costituito oggi dalla rete e dalle sue applicazioni, resta ampiamente insoddisfacente. Proprio la decisione della Corte di giustizia nel caso Google Spain dimostra che i dati personali trattati dai motori di ricerca e da questi indicizzati, assumono caratteristiche del tutto diverse rispetto ai dati personali raccolti in rete e postati nei singoli siti sorgente, creando problemi nuovi e differenti da quelli tradizionali.

Il testo dell'art. 17 del Regolamento, anche nella versione votata dal Parlamento Europeo, non scioglie adeguatamente tutti i nodi legati ai diversi tipi di trattamento dei dati personali operati dai motori di ricerca e dalle molte e diverse applicazioni che i social consentono e consentiranno sempre di più in futuro.

Inoltre, manca una adeguata attenzione al fenomeno delle informazioni poste in rete che riguardano simultaneamente un numero anche elevato di persone diverse, che a diverso titolo possono trovarsi ad assumere, anche senza alcuna loro consapevolezza, la qualifica di interessati. Soggetti che, anche dopo la decisione della Corte di giustizia, non hanno alcuna garanzia di poter intervenire nel procedimento che il gestore del motore di ricerca o del social sia chiamato a fare per valutare la richiesta di cancellazione di un singolo interessato. Infine, nel testo dell'art. 17 manca una adeguata considerazione dei problemi tecnici che il soddisfacimento della richiesta

potrebbe sollevare, anche se un generico e pallido riferimento a questi temi vi è, almeno con riguardo ai dati trattati prima che il Regolamento entri in vigore. È da augurarsi che anche la decisione della Corte di giustizia sul caso Google Spain stimoli ora ad un maggiore approfondimento di questa tematica. Un approfondimento orientato non solo, come è avvenuto sinora, dalla pressione delle lobby ma anche dalla consapevolezza della complessità dei temi in gioco²⁷. È vero che comunque molto potrà fare nel tempo la Commissione avvalendosi del potere ad essa affidato, nel testo attuale del Regolamento, dal paragrafo 9 dell'art. 17. È vero anche, però, che affidare totalmente alla Commissione il compito di sciogliere questi nodi non è opportuno e comunque indebolisce troppo significato e ruolo di questa norma²⁸.

7. *Quale il ruolo delle Autorità dopo la decisione Google Spain e nella realtà della Rete?*

Resta da vedere a questo punto quale possa essere il ruolo che le Autorità garanti potranno esercitare. Già si è detto che la decisione della Corte di giustizia, che pure ha il grande merito di aver isolato e reso chiara

²⁷ Molti di questi problemi sono perfettamente colti da A. MANTELERO, *Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso Google: ricordare e dimenticare nella digital economy*, op. cit.

²⁸ Ci si augura che queste poche e motivate considerazioni non facciano ritenere chi scrive come facente parte di quelli che di recente la Commissaria europea alla giustizia Martine Reicherts ha definito «detrattori che stanno cercando di mettere i bastoni tra le ruote della riforma sulla data protection» e che spesso sono mossi da interessi prevalentemente lobbistici, cfr. M. REICHERTS, «Data protection and right to be forgotten», al *World Library and Information Congress-IFLA*, Lione, Francia, 16-18 agosto 2014, in *Diritto, mercato e tecnologia*, 18 agosto 2014. L'intento di chi scrive è solo che il Regolamento non nasca, per questa parte, già superato dall'evoluzione di quell'enorme ameba mutante che sono i *social* e le applicazioni in rete. Specie dopo la decisione Google Spain dovrebbe essere infatti chiaro a tutti che non si possono più applicare le medesime regole a tutti i trattamenti dati, come se fossero tutti una medesima tipologia di trattamenti, e che le distinzioni, peraltro importanti, che il Regolamento oggi introduce nel rivisitato art. 17 non sono sufficienti. Inoltre dovrebbe essere fatta anche una riflessione più approfondita in ordine alla necessità di rendere il Regolamento flessibile e aperto a auspicabilissime attività regolatorie internazionali, anche in difformità dalle regole in esso oggi contenute. Il rischio, infatti, è che il Regolamento nasca troppo dominato dall'idea di una fortificazione chiusa, con pochi e limitati ponti levatoi, eretta a difesa di una sola regione, l'Unione Europea, in un mondo ogni giorno più globalizzato e quindi sempre più immerso nella 'rete della Rete'.

l'esistenza di questa nuova problematica, è ampiamente insoddisfacente, sia perché non definisce in modo adeguato gli elementi che il gestore deve tener presente sia per accogliere la richiesta dell'interessato, facendo prevalere il suo diritto alla riservatezza, che per respingere la richiesta, facendo prevalere il suo interesse al ritorno economico dell'uso dei dati insieme al più socialmente importante interesse degli utenti a conoscere le informazioni rese accessibili dal motore di ricerca.

Vi sono, poi numerosi problemi tecnici legati alla deindicizzazione dei dati e alla garanzia della loro successiva inaccessibilità²⁹. Problemi che la decisione della Corte neppure affronta.

Proprio queste lacune e questi limiti della decisione sembrano essere i naturali campi nei quali più il ruolo delle Autorità garanti potrà essere prezioso. A tal fine le Autorità dovranno agire in via preventiva e generale, anche attraverso la approvazione di apposite linee guida che orientino i gestori, gli interessati ricorrenti e gli eventuali soggetti di fatto direttamente o indirettamente coinvolti, nonché tutti gli utenti.

È necessario assicurare che la decisione sia interpretata e applicata nel modo più corretto, armonizzato e rispettoso possibile della normativa sulla protezione dei dati personali, anche cercando di dare risposta ai problemi che la sentenza lascia irrisolti o non compiutamente definiti.

Non a caso, del resto, dagli stessi gestori, Google in testa, è pervenuta la richiesta di poter avere con le Autorità un rapporto proattivo, che consenta ad essi di tener conto anche dell'orientamento dei Garanti in sede di valutazione delle richieste e più in generale nell'interpretazione e nell'attuazione della decisione. Né è un caso che la stessa società civile, da ultimo attraverso la già citata lettera della Presidente del *Center for democracy and technology* O'Connor³⁰, abbia chiesto e raccomandato alle Autorità garanti di voler adottare chiare e specifiche linee guida che possano ampliare il più possibile l'area del rispetto della libertà di espressione e definire con chiarezza le procedure di applicazione della decisione, sia rispetto al gestore e all'interessato che rispetto all'eventuale coinvolgimento di soggetti terzi (in particolare gli autori delle notizie postate in rete dalle quali sono tratte le informazioni personali indicizzate dai motori). Inoltre, si chiede di dare indicazioni chiare anche sulle procedure da adottare sia per presentare i ricorsi che per valutare le richieste e comunicare le decisioni, informando non solo gli interessati ma anche gli altri soggetti a diverso titolo coinvolti della rimozione dei dati.

²⁹ Cfr. il contributo di C. COMELLA, *I problemi tecnici della 'de-indicizzazione'*, in questo Volume, *retro*.

³⁰ Cfr. la precedente nota 2.

Le stesse Autorità del resto hanno già anticipato sia col comunicato stampa del 6 giugno che, più estesamente, con quello del 25 luglio, la loro volontà di provvedere a elaborare idonee linee guida entro il prossimo autunno. A seguito della seduta del 25 luglio inoltre le Autorità garanti hanno reso nota anche la lista dei quesiti rivolti in forma scritta a Google e agli altri *provider* finora sentiti dal WP29, e rispetto ai quali dovrebbe essere già stata fornita risposta scritta entro il termine indicato del 30 luglio.

Dalla lista delle domande rivolte e dal tenore dei comunicati stampa anche per la parte relativa agli incontri già avuti con i provider e in base alle prime valutazioni fatte dalle Autorità riguardo al modulo predisposto per formulare le richieste, si può dire che l'attenzione si è fissata in una questa fase essenzialmente sugli aspetti procedurali e sulle modalità adottate per rendere note agli interessati le loro decisioni e l'eventuale avvenuta cancellazione dei dati.

Specifica attenzione è stata dedicata anche a comprendere meglio quale sia per i provider l'ambito di applicazione della sentenza della Corte anche con riguardo all'ambito territoriale nel quale deve essere assicurata la deindicizzazione dei dati.

A queste domande però le Autorità ne hanno aggiunte altre, particolarmente significative, che consentono di capire che esse si stanno muovendo con visione ampia e sulla strada giusta.

È stato chiesto di sapere anche: quali siano i criteri applicati dai gestori per bilanciare il diritto dell'interessato alla cancellazione e l'interesse economico del provider insieme all'interesse degli utenti ad accedere e conoscere le informazioni; quali sono le spiegazioni fondamentali che vengono fornite agli interessati quando si respinge la loro richiesta; se venga data o no notizia agli autori e ai titolari dei siti della avvenuta deindicizzazione delle informazioni postate sui siti fonte e, in caso positivo, su quale base legale si opera.

Vengono chieste inoltre ulteriori cose più specifiche, legate anche ad aspetti tecnici quali: se sia stato approntato un *helping center*; se vi sia su apposita *webpage* l'elenco delle cancellazioni effettuate; se la cancellazione avviene solo tramite modalità elettroniche; se è possibile all'interessato usare la propria lingua nazionale per formulare la richiesta; se le richieste sono catalogate e filtrate per lingua o regione di provenienza; se e quali prove siano richieste per accertare la identità del richiedente e il suo titolo a formulare la richiesta; se sono accettate richieste plurime o se esse devono avere ad oggetto ognuna una singola Url; se la cancellazione dei dati avviene con riferimento solo al nome dell'istante interessato o anche ad

altri indici; se si ritiene o no di poter respingere le richieste formulate da interessati che siano anche autori delle informazioni postate a suo tempo in rete e, nel caso in cui la risposta sia positiva, su quali basi legali si ritiene di operare; se sono stati approntati o no sistemi automatici di analisi e trattamento delle richieste; quali mezzi tecnici si usino per garantire che i dati cancellati non appaiano più attraverso altri chiavi di ricerca; quali siano i servizi assicurati dal sito sorgente considerati di maggior rilievo al fine di garantire che anche su questi la cancellazione del dato abbia pieno effetto; se si preveda che gli utenti del motore di ricerca siano messi al corrente di eventuali cancellazioni operate e, in caso positivo, se questo avvenga per ogni cancellazione o solo per quelle conseguenti all'accoglimento di richieste specifiche, e su quali basi legali si operi nell'uno o nell'altro caso; se si prevede di scambiare la lista delle richieste ricevute e accolte con altri motori di ricerca; se si pensa di creare dei *data base* contenenti le richieste ricevute e quelle accolte o respinte; se si sono adottate iniziative specifiche per implementare l'attuazione piena della decisione, e se si sono riscontrati problemi specifici riguardo particolari richieste già ricevute e trattate.

Infine si chiede ai *provider* di voler fornire alle Autorità specifici punti di contatto attraverso i quali le Autorità possano avere eventuali informazioni su casi specifici di loro interesse.

Lo spettro delle domande è dunque molto molto ampio e dimostra che le Autorità hanno capito perfettamente la dimensione della sfida che la decisione della Corte comporta.

I compiti delle Autorità garanti riunite nel WP29 non può limitarsi a aspetti procedurali o strettamente giuridici, per quanto importanti essi siano. Né può limitarsi soltanto all'ambito territoriale di applicazione da parte del *provider* delle deindicizzazioni relative alle richieste accolte, o alle modalità di coinvolgimento e di avviso (il cosiddetto *notice and take down*) nei confronti di terzi diversi dall'interessato richiedente.

Tutti questi aspetti, sui quali si è appuntata finora l'attenzione prevalente del dibattito dottrinario e mediatico, sono di primaria importanza ma non esauriscono certo il compito che le Autorità sono chiamate a svolgere rispetto ai nuovi orizzonti che la sentenza della Corte di giustizia ha spalancato. Dopo questa decisione è dovere delle Autorità isolare, definire e individuare adeguatamente gli aspetti specifici propri dell'attività del motore di ricerca rispetto alla indicizzazione e messa a disposizione degli utenti dei dati personali raccolti in rete, anche al fine di chiarire i punti che la sentenza della Corte lascia volutamente in sospeso, a cominciare da quello relativo a quali criteri debbano presiedere al giusto bilanciamento

fra i diversi interessi in gioco, al di là di quelli troppo generici e indeterminati contenuti nel punto 97.

Non vi è dubbio, infatti, che anche in questo caso, come molti autori hanno sottolineato, il tendenziale favore per il prevalere del diritto alla riservatezza, e quindi alla deindicizzazione dei dati personali, rispetto all'interesse commerciale del gestore e all'interesse degli utenti a avere le informazioni, deve pur sempre fare i conti col principio di proporzionalità e di adeguatezza del provvedimento.

Il compito delle Autorità va però molto oltre questi aspetti specifici.

Il WP29 deve riprendere l'analisi del rapporto tra attività dei motori di ricerca e protezione dati personali andando oltre la *opinion* n. 148 del 2008 e affrontando finalmente, e a tutto tondo, il tema della pluralità e della specificità dei trattamenti dei dati personali sulla rete, legato all'avvento dei motori di ricerca e dei *social network*.

All'orizzonte si staglia poi il tema, ancora più affascinante di come debbano essere applicate (ed eventualmente innovate) le regole della protezione dei dati personali rispetto a tecnologie di trattamento, utilizzazione, incrocio e archiviazione delle informazioni sempre più sofisticate.

Il riferimento è ovviamente alle tecnologie che incrociano in modo coordinato le tecniche della trasmissione, archiviazione e trattamento a distanza delle informazioni (quelle che vanno genericamente sotto il nome evocativo di *cloud computing*) con quelle che consentono l'archiviazione e il trattamento di quantità sempre più grandi di dati e informazioni per le più diverse finalità (secondo le tecniche legate al nome, ancor più suggestivo e generico, di *Big data*).

Un fenomeno che è ormai realtà diffusa e che consente con misura crescente di trarre informazioni da informazioni, creando nuovi dati e nuove forme di profilazione, conoscenza e controllo delle persone e dei loro comportamenti e relazioni.

È giunta l'ora che le Autorità, muovendo dalla sfida posta dalla decisione su Google Spain, non si limitino più soltanto ad affrontare i problemi, pur importantissimi, di applicazione giuridica delle regole esistenti ma entrino a piedi giunti dentro la nuova, immensa e sconfinata realtà della rete. Una prospettiva nuova, finora affrontata in modo ancora troppo timido e marginale, con provvedimenti settoriali di nicchia³¹, che

³¹ Il WP29 ha dedicato molta e crescente attenzione ai temi della rete, adottando anche numerosi pareri di rilevante importanza. Anche sul tema dei motori di ricerca il gruppo si è pronunciato più volte, prima nel 1998 e poi nel 2006 (cfr. http://www.datenschutz-berlin.de/doc/int/iwgdp/search_engines.pdf) [consultato il 30/09/2014]. Nel 2006 la XXVIII Conferenza internazionale dei Commissari per la protezione dati ha adottato una spe-

offre alle Autorità l'opportunità sconfinata di dimostrare che il loro ruolo va ben oltre la tutela di diritti fondamentali, pur importantissimi della persona e della sua dignità. Proprio perché hanno accumulato una esperienza ormai consolidata in materia di trattamento e protezione dei dati (personali, ma non solo) esse sono sempre più destinate svolgere un ruolo centrale e fondamentale nella società della comunicazione e della informazione globale che segna la nostra epoca. Uomini e donne del pianeta hanno opportunità impensate e impensabili fino ad alcuni decenni fa, ma sono posti anche di fronte a problemi e interrogativi fondamentali per la loro stessa capacità di conservare non solo la libertà ma persino il senso di umanità e di rispetto della dignità delle persone.

È giunta ormai l'ora di far cadere definitivamente il Velo di Maya che da troppi anni anche le Autorità di protezione dati si ostinano a mantenere calato, pur di non prendere fino in fondo atto degli enormi mutamenti che la rete porta con sé.

Un lavoro da fare, che, dopo questa decisione è assolutamente indifferibile, e che è bene sia fatto a fondo e rapidamente. Forse si è ancora in tempo per evitare anche quello che altrimenti appare un rischio sicuro, e cioè che il Regolamento di protezione dei dati personali in discussione sia fin dall'inizio superato da una realtà che anch'esso per troppe parti ignora o vuole ignorare.

Dunque possiamo concludere che la sentenza della Corte di giustizia, anche se ha colto di sorpresa molti, arriva nel momento più opportuno.

Dopo questa sentenza nulla può restare come prima.

Abstract

The ECJ's ruling in Google Spain v. AEPD, Gonzales should be considered

cifica dichiarazione dedicata appunto ai motori di ricerca (cfr. <http://www.privacyconference2006.co.uk/index.asp?PageID=3>). Si sono moltiplicati poi negli anni più recenti i provvedimenti e dichiarazioni relativi ad aspetti specifici, quali la *privacy by design* e i *data breach*. I temi della rete sono stati anche al centro di numerosi Convegni internazionali degli ultimi anni. Tuttavia finora lo sforzo fatto in ambito WP29 è stato sostanzialmente settoriale, mentre di maggiore respiro è stato il lavoro svolto nel c.d. 'Gruppo di Berlino', che essendo una organizzazione parallela alla quale partecipano numerose Autorità e Regolatori di tutti i Paesi, anche extraeuropei, ha per tradizione al centro dei suoi interessi proprio il mondo dell'ICT. Tuttavia finora è mancata la rivendicazione a tutto tondo di un ruolo specifico e proprio delle Autorità connesso ai nuovi problemi di protezione dei dati personali sulla rete.

as a landmark decision in the interpretation of the EU Directive n. 95/46 on data protection in the world of Internet. For the first time, indeed, the Court has considered the search engine provider as a personal data controller, for its private activity of retrieving, indexing, storing and making them accessible, to the general public, of personal data from the web sites. Therefore, an individual has the right to ask for the removal, by the search engine, of links to web pages containing its personal data, which are outdated or irrelevant, without prejudice to the freedom of information — because the activity played by the search engine cannot be assimilated to the press, and the data still remain anyhow available on the original website — and with the only the exception of a compelling public interest, which the Court barely defines. The EU Court also affirmed that a search engine, which has been incorporated outside the EU, shall be anyway considered subjected to the EU Law if the profits of its activity are earned, even by a subsidiary, in an EU Member State.

The paper analyses widely the opinion of the ECJ, mostly underlying that the case does not concern anyway the right to be forgotten and making some insights the role that the EU National Authorities on Data Protection may have to play in implementing the assessment of the Court.

Appendice

1.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

(Grande Sezione)

13 maggio 2014

Sentenza nella causa C131/12,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dall'Audiencia Nacional (Spagna), con decisione del 27 febbraio 2012, pervenuta in cancelleria il 9 marzo 2012, nel procedimento

Google Spain SL,

Google Inc.

contro

Agencia Española de Protección de Datos (AEPD),

Mario Costeja González,

LA CORTE (Grande Sezione),

composta da V. Skouris, presidente, K. Lenaerts, vicepresidente, M. Ileši (relatore),

L. Bay Larsen, T. von Danwitz, M. Safjan, presidenti di sezione, J. Malenovský, E. Levits,

A. Ó Caoimh, A. Arabadjiev, M. Berger, A. Prechal e E. Jaraši nas, giudici,

avvocato generale: N. Jääskinen

cancelliere: M. Ferreira, amministratore principale

vista la fase scritta del procedimento e in seguito all'udienza del 26 febbraio 2013,

considerate le osservazioni presentate:

– per Google Spain SL e Google Inc., da F. González Díaz, J. Baño Fos e B. Holles, abogados;

– per M. Costeja González, da J. Muñoz Rodríguez, abogado;

– per il governo spagnolo, da A. Rubio González, in qualità di agente;

– per il governo ellenico, da E.M. Mamouna e K. Boskovits, in qualità di agenti;

– per il governo italiano, da G. Palmieri, in qualità di agente, assistita da P. Gentili, avvocato dello Stato;

– per il governo austriaco, da G. Kunnert e C. Pesendorfer, in qualità di agenti;

– per il governo polacco, da B. Majczyna e M. Szpunar, in qualità di agenti;

– per la Commissione europea, da I. Martínez del Peral e B. Martenczuk, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 25 giugno 2013, ha pronunciato la seguente

Sentenza

La domanda di pronuncia pregiudiziale verte sull'interpretazione degli articoli 2, lettere

b) e d), 4, paragrafo 1, lettere a) e c), 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31), nonché dell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

2. Tale domanda è stata proposta nell'ambito di una controversia che oppone le società Google Spain SL (in prosieguo: «Google Spain») e Google Inc. all'Agenzia Española de Protección de Datos (AEPD) (Agenzia di protezione dei dati; in prosieguo: l'«AEPD») e al sig. Costeja González, in merito ad una decisione di detta Agenzia che ha accolto la denuncia depositata dal sig. Costeja González contro le due società suddette e ha ordinato a Google Inc. di adottare le misure necessarie per rimuovere dai propri indici alcuni dati personali riguardanti detto interessato e di impedire in futuro l'accesso a tali dati.

Contesto normativo

Diritto dell'Unione

3. La direttiva 95/46 – che, ai sensi del suo articolo 1, ha per oggetto la tutela dei diritti e delle libertà fondamentali delle persone fisiche, e segnatamente del diritto alla vita privata, con riguardo al trattamento dei dati personali, nonché l'eliminazione degli ostacoli alla libera circolazione di tali dati – enuncia, ai considerando 2, 10, da 18 a 20, e 25, quanto segue:

«(2) considerando che i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al (...) benessere degli individui;

(...)

(10) considerando che le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[, firmata a Roma il 4 novembre 1950,] e dai principi generali del diritto comunitario; che pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità;

(...)

(18) considerando che, onde evitare che una persona venga privata della tutela cui

ha diritto in forza della presente direttiva, è necessario che qualsiasi trattamento di dati personali effettuato nella Comunità rispetti la legislazione di uno degli Stati membri; che, a questo proposito, è opportuno assoggettare i trattamenti effettuati da una persona che opera sotto l'autorità del responsabile del trattamento stabilito in uno Stato membro alla legge di tale Stato;

(19) considerando che lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile; che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo; che quando un unico responsabile del trattamento è stabilito nel territorio di diversi Stati membri, in particolare per mezzo di filiali, esso deve assicurare, segnatamente per evitare che le disposizioni vengano eluse, che ognuno degli stabilimenti adempia gli obblighi previsti dalla legge nazionale applicabile alle attività di ciascuno di essi;

(20) considerando che la tutela delle persone prevista dalla presente direttiva non deve essere impedita dal fatto che il responsabile del trattamento sia stabilito in un paese terzo; che, in tal caso, è opportuno che i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto e che siano prese le garanzie necessarie per consentire l'effettivo rispetto dei diritti e degli obblighi previsti dalla presente direttiva;

(...)

(25) considerando che i principi di tutela si esprimono, da un lato, nei vari obblighi a carico delle persone (...) [che trattano dati], obblighi relativi in particolare alla qualità dei dati, alla sicurezza tecnica, alla notificazione all'autorità di controllo, alle circostanze in cui il trattamento può essere effettuato, e, dall'altro, nel diritto delle persone, i cui dati sono oggetto di trattamento, di esserne informate, di poter accedere ai dati, e chiederne la rettifica, o di opporsi al trattamento in talune circostanze».

4. L'articolo 2 della direttiva 95/46 prevede che «[a]i fini [di tale] direttiva si intendono per:

a) “dati personali”: qualsiasi informazione concernente una persona fisica identificata o identificabile (“persona interessata”); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;

b) “trattamento di dati personali” (“trattamento”): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati

personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione;

(...)

d) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;

(...).

5. L'articolo 3 della citata direttiva, intitolato «Campo d'applicazione», enuncia, al paragrafo 1, quanto segue:

«Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi».

6. L'articolo 4 della stessa direttiva, intitolato «Diritto nazionale applicabile», prevede:

«1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:

a) effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile;

b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico;

c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di

transito nel territorio della Comunità europea.

2. Nella fattispecie di cui al paragrafo 1, lettera c), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento».

7. Nell'ambito del capo II della direttiva 95/46, segnatamente nella sezione I, intitolata «Principi relativi alla qualità dei dati», l'articolo 6 dispone quanto segue:

«1. Gli Stati membri dispongono che i dati personali devono essere:

a) trattati lealmente e lecitamente;

b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;

c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;

d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati;

e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.

2. Il responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1».

8. Nel capo II della direttiva 95/46, all'interno della sezione II, intitolata «Principi relativi alla legittimazione del trattamento dei dati», l'articolo 7 recita così:

«Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando:

(...)

f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1».

9. L'articolo 9 della citata direttiva, intitolato «Trattamento di dati personali e libertà d'espressione», ha il seguente tenore:

«Gli Stati membri prevedono, per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, le esenzioni o le deroghe alle disposizioni del presente capo e dei capi IV e VI solo qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione».

10. L'articolo 12 della medesima direttiva, intitolato «Diritto di accesso», così dispone:

«Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento:

(...)

b) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati;

(...)».

11. L'articolo 14 della direttiva 95/46, intitolato «Diritto di opposizione della persona interessata», ha il seguente tenore:

«Gli Stati membri riconoscono alla persona interessata il diritto:

a) almeno nei casi di cui all'articolo 7, lettere e) e f), di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. In caso di opposizione giustificata il trattamento effettuato dal responsabile non può più riguardare tali dati;

(...)».

12. L'articolo 28 di detta direttiva, intitolato «Autorità di controllo», è così formulato:

«1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri.

(...)

3. Ogni autorità di controllo dispone in particolare:

– di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;

– di poteri effettivi d'intervento, come quello (...) di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento (...);

– (...).

È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.

4. Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda.

(...)

6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuiti a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro.

Le autorità di controllo collaborano tra loro nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile.

(...).

Diritto spagnolo

13. La direttiva 95/46 è stata trasposta nell'ordinamento spagnolo mediante la legge organica n. 15/1999, del 13 dicembre 1999, relativa alla tutela dei dati personali (BOE

n. 298, del 14 dicembre 1999, pag. 43088).

Procedimento principale e questioni pregiudiziali

14. Il 5 marzo 2010, il sig. Costeja González, cittadino spagnolo con domicilio in Spagna, ha presentato dinanzi all'AEPD un reclamo contro La Vanguardia Ediciones SL, che pubblica un quotidiano di larga diffusione, soprattutto in Catalogna (Spagna) (in prosieguo: «La Vanguardia»), nonché contro Google Spain e Google Inc. Tale reclamo era fondato sul fatto che, allorché un utente di Internet introduceva il nome del sig. Costeja González nel motore di ricerca del gruppo Google (in prosieguo: «Google Search»), otteneva dei link verso due pagine del quotidiano di La Vanguardia rispettivamente del 19 gennaio e del 9 marzo 1998, sulle quali figurava un annuncio, menzionante il nome del sig. Costeja González, per una vendita all'asta di immobili connessa ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali.

15. Mediante detto reclamo, il sig. Costeja González chiedeva, da un lato, che fosse ordinato a La Vanguardia di sopprimere o modificare le pagine suddette affinché i suoi dati personali non vi comparissero più, oppure di ricorrere a taluni strumenti forniti dai motori di ricerca per proteggere tali dati. Dall'altro lato, egli chiedeva che fosse ordinato a Google Spain o a Google Inc. di eliminare o di occultare i suoi dati personali, in modo che cessassero di comparire tra i risultati di ricerca e non figurassero più nei link di La Vanguardia. Il sig. Costeja González affermava in tale contesto che il pignoramento, che era stato effettuato nei suoi confronti, era stato interamente definito da svariati anni e che la menzione dello stesso era ormai priva di qualsiasi rilevanza.

16. Con decisione del 30 luglio 2010, l'AEPD ha respinto il suddetto reclamo nella parte in cui era diretto contro La Vanguardia, ritenendo che la pubblicazione da parte di quest'ultima delle informazioni in questione fosse legalmente giustificata, dato che aveva avuto luogo su ordine del Ministero del Lavoro e degli Affari sociali e aveva avuto lo scopo di conferire il massimo di pubblicità alla vendita pubblica, al fine di raccogliere il maggior numero di partecipanti all'asta.

17. Detto reclamo è stato invece accolto nella parte in cui era diretto contro Google Spain e Google Inc. L'AEPD ha considerato in proposito che i gestori di motori di ricerca sono assoggettati alla normativa in materia di protezione dei dati, dato che essi effettuano un trattamento di dati per il quale sono responsabili e agiscono quali intermediari della società dell'informazione. L'AEPD ha ritenuto di essere autorizzata ad ordinare la rimozione dei dati nonché il divieto di accesso a taluni dati da parte dei gestori di motori di ricerca, qualora essa ritenga che la localizzazione e la diffusione degli stessi possano ledere il diritto fondamentale alla protezione dei dati e la dignità delle persone in senso ampio, ciò che includerebbe anche la semplice volontà della persona interessata che tali dati non

siano conosciuti da terzi. L'AEPD ha affermato che tale obbligo può incombere direttamente ai gestori di motori di ricerca, senza che sia necessario cancellare i dati o le informazioni dal sito web in cui questi compaiono, segnatamente quando il mantenimento di tali informazioni nel sito in questione sia giustificato da una norma di legge.

18. Google Spain e Google Inc. hanno proposto due ricorsi separati contro la decisione di cui sopra dinanzi all'Audiencia Nacional, dei quali quest'ultima ha disposto la riunione.

19. Detto giudice chiarisce nella decisione di rinvio che i ricorsi sopra menzionati portano a chiedersi quali obblighi incombono ai gestori di motori di ricerca per la tutela dei dati personali delle persone interessate, le quali non desiderino che alcune informazioni, pubblicate sui siti web di terzi e contenenti loro dati personali che consentono di collegare ad esse dette informazioni, vengano localizzate, indicizzate e messe a disposizione degli utenti di Internet in modo indefinito. La risposta a tale quesito dipenderebbe dal modo in cui la direttiva 95/46 deve essere interpretata nel contesto di queste tecnologie che sono apparse dopo la sua pubblicazione.

20. Alla luce di tali considerazioni, l'Audiencia Nacional ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Per quanto concerne l'ambito territoriale di applicazione della direttiva [95/46] e, di conseguenza, della normativa spagnola sulla protezione dei dati, si chiede:

a) Se debba ritenersi che esista uno “stabilimento” ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva [95/46], qualora ricorrano una o più delle seguenti circostanze:

– l'impresa che gestisce il motore di ricerca apre in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca e l'attività della quale si dirige agli abitanti di tale Stato;

o

– la società madre designa una filiale situata in tale Stato membro come suo rappresentante e responsabile del trattamento di due file specifici contenenti i dati dei clienti che hanno stipulato contratti con detta società per la fornitura di servizi pubblicitari;

o

– la succursale o la filiale stabilita in uno Stato membro trasmette alla società madre, avente sede al di fuori dell'Unione europea, i reclami e le ingiunzioni che le vengono presentati tanto dalle persone interessate quanto dalle autorità competenti perché

sia rispettato il diritto alla protezione dei dati, anche quando tale collaborazione abbia carattere volontario.

b) Se l'articolo 4, paragrafo 1, lettera c), della direttiva [95/46] debba essere interpretato nel senso che si configura un "ricorso a strumenti situati nel territorio di detto Stato membro" qualora un motore di ricerca:

– utilizzi dei "web spiders" o dei crawler per localizzare e indicizzare le informazioni contenute in pagine web alloggiate su server situati in tale Stato membro

o

– utilizzi un nome di dominio proprio di uno Stato membro e indirizzi le ricerche e i risultati in funzione della lingua di tale Stato membro.

c) Se possa considerarsi come un ricorso a strumenti, ai sensi dell'articolo 4, paragrafo 1, lettera c), della direttiva [95/46], la memorizzazione temporanea delle informazioni indicizzate dai motori di ricerca su Internet. In caso di risposta affermativa a quest'ultimo quesito, se si possa ritenere soddisfatto tale criterio di collegamento quando l'impresa si rifiuti di rivelare il luogo in cui archivia detti indici, adducendo ragioni di concorrenza.

d) A prescindere dalla risposta ai precedenti quesiti, e specialmente nel caso in cui la Corte ritenesse inapplicabili i criteri di collegamento previsti dall'articolo 4 della direttiva [95/46]:

Se, alla luce dell'articolo 8 della [Carta], la direttiva [95/46] debba essere applicata nello Stato membro nel quale si trova il centro di gravità del conflitto e nel quale è possibile ottenere una tutela più efficace dei diritti dei cittadini dell'Unione (...).

2) Per quanto concerne l'attività dei motori di ricerca quali fornitori di contenuti in relazione alla direttiva [95/46], si chiede:

a) Riguardo all'attività [di Google Search] quale fornitore di contenuti, consistente nel localizzare le informazioni pubblicate o messe in rete da terzi, nell'indicizzarle in maniera automatica, nel memorizzarle temporaneamente e infine nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, qualora tali informazioni contengano dati personali di terzi:

Se un'attività come quella descritta debba considerarsi rientrante nella nozione di "trattamento di dati" ai sensi dell'articolo 2, lettera b), della direttiva [95/46].

b) In caso di risposta affermativa al quesito precedente, e sempre con riferimento ad un'attività come quella sopra descritta:

Se l'articolo 2, lettera d), della direttiva [95/46] debba essere interpretato nel senso che la società che gestisce [Google Search] deve essere considerata "responsabile del trattamento" dei dati personali contenuti nelle pagine web da essa indicizzate.

c) In caso di risposta affermativa al quesito precedente:

Se l'[AEPD], al fine di tutelare i diritti enunciati agli articoli 12, lettera b), e 14, [primo comma,] lettera a), della direttiva [95/46], possa ordinare direttamente [a Google Search] di rimuovere dai propri indici un'informazione pubblicata da terzi, senza rivolgersi previamente o simultaneamente al titolare della pagina web in cui è inserita tale informazione.

d) In caso di risposta affermativa al quesito precedente:

Se i motori di ricerca siano sollevati dall'obbligo di rispettare i diritti di cui sopra qualora l'informazione contenente i dati personali sia stata lecitamente pubblicata da terzi e rimanga sulla pagina web di origine.

3) Per quanto concerne la portata del diritto di cancellazione e/o opposizione al trattamento di dati in relazione al diritto all'oblio, si chiede:

Se si debba ritenere che i diritti di cancellazione e congelamento dei dati, disciplinati dall'articolo 12, lettera b), e il diritto di opposizione al loro trattamento, regolato dall'articolo 14, [primo comma,] lettera a), della direttiva [95/46], implichino che l'interessato può rivolgersi ai motori di ricerca per impedire l'indicizzazione delle informazioni riguardanti la sua persona pubblicate su pagine web di terzi, facendo valere la propria volontà che tali informazioni non siano conosciute dagli utenti di Internet, ove egli reputi che la loro divulgazione possa arrecargli pregiudizio o desideri che tali informazioni siano dimenticate, anche quando si tratti di informazioni pubblicate da terzi lecitamente».

Sulle questioni pregiudiziali

Sulla seconda questione, lettere a) e b), concernente l'ambito di applicazione materiale della direttiva 95/46

21. Con la sua seconda questione, lettere a) e b), da esaminarsi per prima, il giudice del rinvio chiede, in sostanza, se l'articolo 2, lettera b), della direttiva 95/46 debba essere interpretato nel senso che l'attività di un motore di ricerca quale fornitore di contenuti, consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle

a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», ai sensi della disposizione suddetta, qualora tali informazioni contengano dati personali. In caso di risposta affermativa, il giudice del rinvio desidera inoltre sapere se il citato articolo 2, lettera d), debba essere interpretato nel senso che il gestore di un motore di ricerca deve essere considerato come il «responsabile» del suddetto trattamento di dati personali, ai sensi di quest'ultima disposizione.

22. Secondo Google Spain e Google Inc., l'attività dei motori di ricerca non può essere considerata quale trattamento dei dati che appaiono sulle pagine web di terzi visualizzate nell'elenco dei risultati della ricerca, dato che detti motori di ricerca trattano le informazioni accessibili su Internet nel loro insieme senza operare una selezione tra i dati personali e le altre informazioni. Inoltre, anche supponendo che tale attività debba essere qualificata come «trattamento di dati», il gestore di un motore di ricerca non può essere considerato come «responsabile» di tale trattamento, dal momento che egli non ha conoscenza dei dati in questione e non esercita alcun controllo su di essi.

23. Per contro, il sig. Costeja González, i governi spagnolo, italiano, austriaco e polacco, nonché la Commissione europea, ritengono che l'attività suddetta implichi all'evidenza un «trattamento di dati» nel senso di cui alla direttiva 95/46, il quale si distingue dal trattamento di dati ad opera degli editori di siti web e persegue obiettivi diversi rispetto a quelli di quest'ultimo. Il gestore di un motore di ricerca sarebbe «responsabile» del trattamento dei dati da questo effettuato, essendo detto gestore a determinare le finalità e gli strumenti di tale trattamento.

24. Secondo il governo ellenico, l'attività in questione costituisce un «trattamento» siffatto, ma poiché i motori di ricerca fungono da semplici intermediari, le imprese che li gestiscono non possono essere considerate «responsabili», ad eccezione del caso in cui esse memorizzino dei dati in una «memoria intermedia» o una «memoria cache» per un periodo di tempo superiore a quanto tecnicamente necessario.

25. A questo proposito occorre rilevare come l'articolo 2, lettera b), della direttiva 95/46 definisca il «trattamento di dati personali» come «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione».

26. Per quanto riguarda in particolare Internet, la Corte ha già avuto modo di constatare che l'operazione consistente nel far comparire su una pagina Internet dati perso-

nali va considerata come un «trattamento» siffatto ai sensi dell'articolo 2, lettera b), della direttiva 95/46 (v. sentenza Lindqvist, C101/01, EU:C:2003:596, punto 25).

27. Per quanto concerne l'attività in esame nel procedimento principale, non è contestato che tra i dati trovati, indicizzati, memorizzati dai motori di ricerca e messi a disposizione degli utilizzatori di questi ultimi sono presenti anche informazioni riguardanti persone fisiche identificate o identificabili, e dunque «dati personali» ai sensi dell'articolo 2, lettera a), della direttiva citata.

28. Pertanto, occorre constatare che, esplorando Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni ivi pubblicate, il gestore di un motore di ricerca «raccolge» dati siffatti, che egli «estrae», «registra» e «organizza» successivamente nell'ambito dei suoi programmi di indicizzazione, «conserva» nei suoi server e, eventualmente, «comunica» e «mette a disposizione» dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche. Poiché tali operazioni sono contemplate in maniera esplicita e incondizionata all'articolo 2, lettera b), della direttiva 95/46, esse devono essere qualificate come «trattamento» ai sensi di tale disposizione, senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali.

29. La constatazione di cui sopra non viene invalidata neppure dal fatto che tali dati abbiano già costituito l'oggetto di una pubblicazione su Internet e non vengano modificati dal suddetto motore di ricerca.

30. Infatti, la Corte ha già constatato che le operazioni contemplate dall'articolo 2, lettera b), della direttiva 95/46 devono essere considerate come un trattamento siffatto anche nell'ipotesi in cui riguardino esclusivamente informazioni già pubblicate tali e quali nei media. La Corte ha infatti rilevato, a questo proposito, che una deroga generale all'applicazione della direttiva 95/46 in un'ipotesi siffatta priverebbe in larga parte del suo significato tale direttiva (v., in tal senso, sentenza Satakunnan Markkinapörssi e Satamedia, C73/07, EU:C:2008:727, punti 48 e 49).

31. Inoltre, discende dalla definizione contenuta nell'articolo 2, lettera b), della direttiva 95/46 che, se indubbiamente la modificazione di dati personali costituisce un trattamento ai sensi della direttiva stessa, le altre operazioni menzionate in tale disposizione non esigono affatto, invece, che i dati suddetti vengano modificati.

32. Quanto alla questione se il gestore di un motore di ricerca debba o no essere considerato come il «responsabile del trattamento» dei dati personali effettuato da tale motore nell'ambito di un'attività come quella oggetto del procedimento principale, occorre ricordare che l'articolo 2, lettera d), della direttiva 95/46 definisce detto responsabi-

le come «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali».

33. Orbene, è il gestore del motore di ricerca a determinare le finalità e gli strumenti di tale attività e dunque del trattamento di dati personali che egli stesso effettua nell'ambito dell'attività medesima, ed è di conseguenza lui a dover essere considerato come il «responsabile» di tale trattamento a norma del citato articolo 2, lettera d).

34. Inoltre, occorre constatare che sarebbe contrario non soltanto al chiaro tenore letterale di tale disposizione, ma anche alla sua finalità – consistente nel garantire, mediante un'ampia definizione della nozione di «responsabile», una tutela efficace e completa delle persone interessate – il fatto di escludere dalla nozione di cui sopra il gestore di un motore di ricerca per il motivo che egli non esercita alcun controllo sui dati personali pubblicati sulle pagine web di terzi.

35. A questo proposito, occorre sottolineare che il trattamento di dati personali effettuato nell'ambito dell'attività di un motore di ricerca si distingue da e si aggiunge a quello effettuato dagli editori di siti web, consistente nel far apparire tali dati su una pagina Internet.

36. Inoltre, è pacifico che tale attività dei motori di ricerca svolge un ruolo decisivo nella diffusione globale dei dati suddetti, in quanto rende accessibili questi ultimi a qualsiasi utente di Internet che effettui una ricerca a partire dal nome della persona interessata, anche a quegli utenti che non avrebbero altrimenti trovato la pagina web su cui questi stessi dati sono pubblicati.

37. Per di più, l'organizzazione e l'aggregazione delle informazioni pubblicate su Internet, realizzate dai motori di ricerca allo scopo di facilitare ai loro utenti l'accesso a dette informazioni, possono avere come effetto che tali utenti, quando la loro ricerca viene effettuata a partire dal nome di una persona fisica, ottengono attraverso l'elenco di risultati una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che consente loro di stabilire un profilo più o meno dettagliato di quest'ultima.

38. Pertanto, nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46, affinché le garanzie previste da

quest'ultima possano sviluppare pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata.

39. Infine, la circostanza che gli editori di siti web abbiano la facoltà di indicare ai gestori di motori di ricerca, con l'aiuto segnatamente di protocolli di esclusione come «robot.txt» o di codici come «noindex» o «noarchive», il loro desiderio che una determinata informazione, pubblicata sul loro sito, venga esclusa in tutto o in parte dagli indici automatici di detti motori di ricerca, non significa che la mancanza di un'indicazione siffatta da parte di questi editori liberi il gestore di un motore di ricerca dalla sua responsabilità per il trattamento dei dati personali che egli effettua nell'ambito dell'attività del motore stesso.

40. Infatti, tale circostanza non modifica il fatto che le finalità e gli strumenti del citato trattamento sono determinati da detto gestore. Inoltre, anche supponendo che la summenzionata facoltà degli editori di siti web significhi che costoro determinano insieme con il suddetto gestore gli strumenti di tale trattamento, tale circostanza nulla toglierebbe alla responsabilità di quest'ultimo, dato che l'articolo 2, lettera d), della direttiva 95/46 prevede espressamente che tale determinazione possa essere effettuata «da solo o insieme ad altri».

41. Alla luce di quanto sopra esposto, occorre rispondere alla seconda questione, lettere a) e b), dichiarando che l'articolo 2, lettere b) e d), della direttiva 95/46 deve essere interpretato nel senso che, da un lato, l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», ai sensi del citato articolo 2, lettera b), qualora tali informazioni contengano dati personali, e che, dall'altro lato, il gestore di detto motore di ricerca deve essere considerato come il «responsabile» del trattamento summenzionato, ai sensi dell'articolo 2, lettera d), di cui sopra.

Sulla prima questione, lettere da a) a d), concernente l'ambito di applicazione territoriale della direttiva 95/46

42. Con la sua prima questione, lettere da a) a d), il giudice del rinvio mira a stabilire se sia possibile applicare la normativa nazionale di recepimento della direttiva 95/46 in circostanze quali quelle in esame nel procedimento principale.

43. In tale contesto, il giudice del rinvio ha accertato i seguenti fatti:

– Google Search viene proposto a livello mondiale tramite il sito web «www.google.com». In numerosi Stati esistono versioni locali adattate alla lingua nazionale. La versione in lingua spagnola di Google Search viene proposta tramite il sito web «www.google.es», registrato dal 16 settembre 2003. Google Search è uno dei motori di ricerca più utilizzati in Spagna.

– Google Search è gestito da Google Inc., che è la società madre del gruppo Google e la cui sede sociale si trova negli Stati Uniti.

– Google Search indicizza i siti web del mondo intero, e tra questi i siti ubicati in Spagna. Le informazioni indicizzate dai suoi «web spiders» o dai suoi crawler, ossia programmi informatici utilizzati per reperire e scandagliare il contenuto delle pagine web in modo metodico e automatizzato, vengono memorizzate temporaneamente in server dei quali si ignora lo Stato di ubicazione, informazione questa che viene mantenuta segreta per ragioni di concorrenza.

– Google Search non si limita a dare accesso ai contenuti ospitati sui siti web indicizzati, ma sfrutta tale attività per includere, dietro pagamento, pubblicità associate ai termini di ricerca introdotti dagli utenti di Internet, a beneficio di imprese che desiderano utilizzare tale mezzo per offrire i loro beni o servizi a tali utenti.

– Il gruppo Google utilizza la propria filiale Google Spain per la promozione delle vendite di spazi pubblicitari generati sul sito web «www.google.com». Google Spain, che è stata costituita il 3 settembre 2003 e che gode di personalità giuridica autonoma, ha la propria sede sociale a Madrid (Spagna). Essa sviluppa le proprie attività essenzialmente a destinazione delle imprese basate in Spagna, operando quale agente commerciale del gruppo suddetto in tale Stato membro. Il suo oggetto sociale consiste nel promuovere, facilitare ed effettuare la vendita di prodotti e di servizi di pubblicità online a terzi, nonché il marketing di questa pubblicità.

– Google Inc. ha designato Google Spain come responsabile del trattamento, in Spagna, di due file registrati da Google Inc. presso l'AEPD, tenendo presente che tali file hanno lo scopo di contenere i dati personali dei clienti che hanno concluso contratti di servizi pubblicitari con Google Inc.

44. In concreto, il giudice del rinvio si interroga, in via principale, in merito alla nozione di «stabilimento», ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46, e a quella di «ricorso a strumenti situati nel territorio di detto Stato membro», ai sensi dell'articolo 4, paragrafo 1, lettera c), della medesima direttiva.

Sulla prima questione, lettera a)

45. Con la sua prima questione, lettera a), il giudice del rinvio chiede, in sostanza, se l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 debba essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione di cui sopra, qualora una o più delle seguenti tre condizioni siano soddisfatte:

- il gestore di un motore di ricerca apre in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca e l'attività della quale si dirige agli abitanti di tale Stato, oppure
- la società madre designa una filiale situata in tale Stato membro come suo rappresentante e responsabile del trattamento di due file specifici contenenti i dati dei clienti che hanno stipulato contratti con detta società per la fornitura di servizi pubblicitari, oppure
- la succursale o la filiale stabilita in uno Stato membro trasmette alla società madre, avente sede al di fuori dell'Unione, i reclami e le ingiunzioni che le vengono presentati tanto dalle persone interessate quanto dalle autorità competenti perché sia rispettato il diritto alla protezione dei dati personali, anche quando tale collaborazione abbia carattere volontario.

46. Per quanto riguarda la prima di queste tre condizioni, il giudice del rinvio rileva che Google Search è gestito e amministrato da Google Inc., e che non è dimostrato che Google Spain realizzi in Spagna un'attività direttamente connessa all'indicizzazione o alla memorizzazione di informazioni o di dati contenuti nei siti web di terzi. Tuttavia, l'attività di promozione e di vendita degli spazi pubblicitari, di cui si occupa Google Spain per la Spagna, costituirebbe la parte essenziale dell'attività commerciale del gruppo Google e potrebbe essere considerata come strettamente connessa a Google Search.

47. Il sig. Costeja González, i governi spagnolo, italiano, austriaco e polacco, nonché la Commissione, ritengono che, tenuto conto del nesso inscindibile tra l'attività del motore di ricerca gestito da Google Inc. e quella di Google Spain, quest'ultima debba essere considerata come uno stabilimento della prima, nel contesto delle cui attività viene effettuato il trattamento di dati personali. Invece, secondo Google Spain, Google Inc. ed il governo ellenico, l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 non trova applicazione nell'ipotesi corrispondente alla prima delle tre condizioni elencate dal giudice del rinvio.

48. A questo proposito occorre anzitutto rilevare che il considerando 19 della direttiva 95/46 precisa che «lo stabilimento nel territorio di uno Stato membro implica l'e-

servizio effettivo e reale dell'attività mediante un'organizzazione stabile», e «che la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo».

49. Orbene, non è contestato che Google Spain si dedica all'esercizio effettivo e reale di un'attività mediante un'organizzazione stabile in Spagna. Essendo inoltre dotata di una personalità giuridica propria, detta società costituisce in tal modo una filiale di Google Inc. nel territorio spagnolo e, di conseguenza, uno «stabilimento» ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46.

50. Al fine di soddisfare il criterio fissato da questa disposizione, è altresì necessario che il trattamento di dati personali ad opera del responsabile dello stesso venga «effettuato nel contesto delle attività» di uno stabilimento di questo responsabile nel territorio di uno Stato membro.

51. Google Spain e Google Inc. negano che tale situazione sussista nel caso di specie, dal momento che il trattamento di dati personali in esame nel procedimento principale viene effettuato esclusivamente da Google Inc., che gestisce Google Search senza alcun intervento da parte di Google Spain, la cui attività si limita alla fornitura di un sostegno all'attività pubblicitaria del gruppo Google, che si differenzia dal suo servizio di motore di ricerca.

52. Tuttavia, come sottolineato in particolare dal governo spagnolo e dalla Commissione, l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 non esige che il trattamento di dati personali in questione venga effettuato «dallo» stesso stabilimento interessato, bensì soltanto che venga effettuato «nel contesto delle attività» di quest'ultimo.

53. Inoltre, alla luce dell'obiettivo della direttiva 95/46 di garantire una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, con riguardo al trattamento dei dati personali, l'espressione suddetta non può ricevere un'interpretazione restrittiva (v., per analogia, sentenza L'Oréal e a., C324/09, EU:C:2011:474, punti 62 e 63).

54. In tali circostanze, occorre rilevare che risulta in particolare dai considerando da 18 a 20 e dall'articolo 4 della direttiva 95/46 che il legislatore dell'Unione ha inteso evitare che una persona venga esclusa dalla protezione garantita da tale direttiva e che tale protezione venga elusa, prevedendo a tal fine un ambito di applicazione territoriale particolarmente esteso.

55. Tenuto conto di tale obiettivo della direttiva 95/46 e del tenore letterale del suo articolo 4, paragrafo 1, lettera a), occorre affermare che il trattamento di dati personali

realizzato per le esigenze di servizio di un motore di ricerca come Google Search, il quale venga gestito da un'impresa con sede in uno Stato terzo ma avente uno stabilimento in uno Stato membro, viene effettuato «nel contesto delle attività» di tale stabilimento qualora quest'ultimo sia destinato a garantire, in tale Stato membro, la promozione e la vendita degli spazi pubblicitari proposti dal suddetto motore di ricerca, che servono a rendere redditizio il servizio offerto da quest'ultimo.

56. Infatti, in circostanze del genere, le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio e che tale motore è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività.

57. A questo proposito occorre ricordare che, come si è precisato ai punti da 26 a 28 della presente sentenza, la visualizzazione stessa di dati personali su una pagina di risultati di una ricerca costituisce un trattamento di dati personali. Orbene, poiché la suddetta visualizzazione di risultati è accompagnata, sulla stessa pagina, da quella di pubblicità correlate ai termini di ricerca, è giocoforza constatare che il trattamento di dati personali in questione viene effettuato nel contesto dell'attività pubblicitaria e commerciale dello stabilimento del responsabile del trattamento nel territorio di uno Stato membro, nella fattispecie il territorio spagnolo.

58. Date tali circostanze, non si può accettare che il trattamento di dati personali effettuato per le esigenze del funzionamento del suddetto motore di ricerca venga sottratto agli obblighi e alle garanzie previsti dalla direttiva 95/46, ciò che pregiudicherebbe l'effetto utile di quest'ultima e la tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche che detta direttiva mira a garantire (v., per analogia, sentenza *L'Oréal e a.*, EU:C:2011:474, punti 62 e 63), segnatamente il diritto al rispetto della loro vita privata, con riguardo al trattamento dei dati personali, al quale detta direttiva riconosce un'importanza particolare, come confermato segnatamente dall'articolo 1, paragrafo 1, e dai considerando 2 e 10 della direttiva medesima (v., in tal senso, sentenze *Österreichischer Rundfunk e a.*, C465/00, C138/01 e C139/01, EU:C:2003:294, punto 70; *Rijkeboer*, C553/07, EU:C:2009:293, punto 47, nonché *IPI*, C473/12, EU:C:2013:715, punto 28 e la giurisprudenza ivi citata).

59. Dal momento che la prima delle tre condizioni elencate dal giudice del rinvio è sufficiente di per sé sola per concludere che uno stabilimento come Google Spain soddisfa il criterio previsto dall'articolo 4, paragrafo 1, lettera a), della direttiva 95/46, non è necessario esaminare le altre due condizioni.

60. Alla luce delle considerazioni di cui sopra, occorre rispondere alla prima que-

stione, lettera a), dichiarando che l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro.

Sulla prima questione, lettere da b) a d)

61. Tenuto conto della soluzione data alla prima questione, lettera a), non vi è luogo a rispondere alla prima questione, lettere da b) a d).

Sulla seconda questione, lettere c) e d), concernente l'estensione della responsabilità del gestore di un motore di ricerca ai sensi della direttiva 95/46

62. Con la sua seconda questione, lettere c) e d), il giudice del rinvio chiede, in sostanza, se gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 debbano essere interpretati nel senso che, per rispettare i diritti previsti da tali disposizioni, il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine sia di per sé lecita.

63. Google Spain e Google Inc. ritengono che, in virtù del principio di proporzionalità, qualsiasi domanda diretta alla soppressione di informazioni debba essere indirizzata all'editore del sito web interessato, in quanto quest'ultimo è colui che assume la responsabilità di rendere pubbliche le informazioni, che è in grado di valutare la liceità di tale pubblicazione e che dispone dei mezzi più efficaci e meno restrittivi per rendere inaccessibili le informazioni stesse. Inoltre, imporre al gestore di un motore di ricerca di rimuovere dai propri indici informazioni pubblicate su Internet non terrebbe sufficientemente conto dei diritti fondamentali degli editori di siti web, degli altri utenti di Internet, nonché dello stesso gestore.

64. Secondo il governo austriaco, un'autorità di controllo nazionale può ordinare a tale gestore di cancellare dai propri archivi informazioni pubblicate da terzi unicamente nel caso in cui l'illiceità o l'inesattezza dei dati in questione sia stata previamente constatata o la persona interessata abbia presentato con successo un'opposizione dinanzi all'editore del sito web sul quale tali informazioni sono state pubblicate.

65. Il sig. Costeja González, i governi spagnolo, italiano e polacco, nonché la Commissione, ritengono che l'autorità nazionale possa ordinare direttamente al gestore di un motore di ricerca di rimuovere dai propri indici e dalla propria memoria intermedia informazioni contenenti dati personali pubblicati da terzi, senza doversi rivolgere previamente o simultaneamente all'editore della pagina web nella quale compaiono tali informazioni. Oltre a ciò, ad avviso del sig. Costeja González, dei governi spagnolo e italiano nonché della Commissione, la circostanza che le informazioni suddette siano state pubblicate in modo lecito e ancora compaiano sulla pagina web d'origine non incide sugli obblighi incombenti a detto gestore in forza della direttiva 95/46. Invece, per il governo polacco, tale circostanza è idonea a liberare il gestore del motore di ricerca dai propri obblighi.

66. In via preliminare, occorre ricordare che, come risulta dall'articolo 1 e dal considerando 10 della direttiva 95/46, quest'ultima mira a garantire un livello elevato di protezione delle libertà e dei diritti fondamentali delle persone fisiche, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali (v., in tal senso, sentenza IPI, EU:C:2013:715, punto 28).

67. A mente del considerando 25 della direttiva 95/46, i principi di tutela previsti da quest'ultima si esprimono, da un lato, nei vari obblighi a carico dei soggetti che trattano dati – obblighi relativi in particolare alla qualità dei dati, alla sicurezza tecnica, alla notificazione all'autorità di controllo, alle circostanze in cui il trattamento può essere effettuato – e, dall'altro, nel diritto delle persone, i cui dati sono oggetto di trattamento, di esserne informate, di poter accedere ai dati e di poterne chiedere la rettifica, o anche di opporsi al trattamento in talune circostanze.

68. La Corte ha già statuito che le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto alla vita privata, devono necessariamente essere interpretate alla luce dei diritti fondamentali che, secondo una costante giurisprudenza, formano parte integrante dei principi generali del diritto di cui la Corte garantisce l'osservanza e che sono ormai iscritti nella Carta (v., in particolare, sentenze Connolly/Commissione, C274/99 P, EU:C:2001:127, punto 37, nonché Österreichischer Rundfunk e a., EU:C:2003:294, punto 68).

69. In tal senso, l'articolo 7 della Carta garantisce il diritto al rispetto della vita privata, mentre l'articolo 8 della Carta proclama espressamente il diritto alla protezione dei dati personali. I paragrafi 2 e 3 di quest'ultimo articolo precisano che i dati suddetti devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la

rettifica, e che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente. Tali prescrizioni ricevono attuazione in particolare mediante gli articoli 6, 7, 12, 14 e 28 della direttiva 95/46.

70. Quanto all'articolo 12, lettera b), della direttiva 95/46, esso dispone che gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento, a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non sia conforme alle disposizioni di questa direttiva, in particolare a causa del carattere incompleto o inesatto dei dati. Poiché quest'ultima precisazione relativa all'ipotesi del mancato rispetto di talune prescrizioni dettate dall'articolo 6, paragrafo 1, lettera d), della direttiva 95/46 risulta avere carattere esemplificativo e non esaustivo, ne consegue che la non conformità del trattamento, atta a conferire alla persona interessata il diritto garantito dall'articolo 12, lettera b), di tale direttiva, può derivare anche dal mancato rispetto delle altre condizioni di liceità imposte da quest'ultima al trattamento di dati personali.

71. A questo proposito occorre ricordare che, fatte salve le deroghe ammesse ai sensi dell'articolo 13 della direttiva 95/46, qualsiasi trattamento di dati personali deve, da un lato, essere conforme ai principi relativi alla qualità dei dati, enunciati all'articolo 6 di detta direttiva, e, dall'altro, rispondere ad uno dei principi relativi alla legittimazione dei trattamenti di dati, elencati all'articolo 7 della direttiva stessa (v. sentenze *Österreichischer Rundfunk e a.*, EU:C:2003:294, punto 65; *ASNEF e FECEMD*, C468/10 e C469/10, EU:C:2011:777, punto 26, nonché *Worten*, C342/12, EU:C:2013:355, punto 33).

72. A mente del citato articolo 6, e fatte salve le disposizioni specifiche che gli Stati membri possono prevedere per trattamenti a scopi storici, statistici o scientifici, spetta al responsabile del trattamento garantire che i dati personali siano «trattati lealmente e lecitamente», che vengano «rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità», che siano «adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati», che siano «esatti e, se necessario, aggiornati» e, infine, che siano «conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati». In tale contesto, detto responsabile deve prendere tutte le misure ragionevoli affinché i dati che non soddisfano le prescrizioni dettate dalla disposizione suddetta vengano cancellati o rettificati.

73. Quanto alla legittimazione, ai sensi dell'articolo 7 della direttiva 95/46, di un trattamento come quello oggetto del procedimento principale effettuato dal gestore di un motore di ricerca, esso può ricadere sotto il motivo contemplato dal citato articolo 7, alla

lettera f).

74. Tale disposizione consente il trattamento di dati personali allorché questo è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del terzo o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata – segnatamente il suo diritto al rispetto della sua vita privata con riguardo al trattamento dei dati personali –, i quali richiedono una tutela ai sensi dell'articolo 1, paragrafo 1, di detta direttiva. L'applicazione del citato articolo 7, lettera f), esige dunque una ponderazione dei contrapposti diritti e interessi in gioco, nell'ambito della quale si deve tener conto dell'importanza dei diritti della persona interessata risultanti dagli articoli 7 e 8 della Carta (v. sentenza ASNEF e FECEMD, EU:C:2011:777, punti 38 e 40).

75. Se dunque la conformità del trattamento di dati agli articoli 6 e 7, lettera f), della direttiva 95/46 può essere verificata nell'ambito di una domanda ai sensi dell'articolo 12, lettera b), di quest'ultima, la persona interessata può inoltre avvalersi, a determinate condizioni, del diritto di opposizione previsto dall'articolo 14, primo comma, lettera a), della medesima direttiva.

76. Ai sensi di tale articolo 14, primo comma, lettera a), gli Stati membri riconoscono alla persona interessata il diritto – almeno nei casi di cui all'articolo 7, lettere e) e f), della citata direttiva – di opporsi in qualsiasi momento, per motivi preminenti e legittimi derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. La ponderazione da effettuarsi nell'ambito di tale articolo 14, primo comma, lettera a), permette così di tener conto in modo più specifico di tutte le circostanze caratterizzanti la situazione concreta della persona interessata. In caso di opposizione giustificata, il trattamento messo in atto dal responsabile di quest'ultimo non può più riguardare tali dati.

77. Le domande ai sensi degli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 possono essere direttamente presentate dalla persona interessata al responsabile del trattamento, il quale deve in tal caso procedere al debito esame della loro fondatezza e, eventualmente, porre fine al trattamento dei dati in questione. Qualora il responsabile del trattamento non dia seguito a tali domande, la persona interessata può adire l'autorità di controllo o l'autorità giudiziaria affinché queste effettuino le verifiche necessarie e ordinino al suddetto responsabile l'adozione di misure precise conseguenti.

78. A questo proposito occorre rilevare che dall'articolo 28, paragrafi 3 e 4, della direttiva 95/46 risulta che qualsiasi persona può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali, e che tale autorità dispone di poteri investigativi e di poteri effettivi di

intervento che le consentono di ordinare in particolare il congelamento, la cancellazione o la distruzione di dati, oppure di vietare a titolo provvisorio o definitivo un trattamento.

79. È alla luce di tali considerazioni che occorre interpretare e applicare le disposizioni della direttiva 95/46 disciplinanti i diritti della persona interessata allorché quest'ultima presenta all'autorità di controllo o all'autorità giudiziaria una domanda quale quella oggetto del procedimento a quo.

80. A questo proposito occorre anzitutto rilevare che, come si è constatato ai punti da 36 a 38 della presente sentenza, un trattamento di dati personali, quale quello in esame nel procedimento principale, effettuato dal gestore di un motore di ricerca, può incidere significativamente sui diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, nel caso in cui la ricerca con l'aiuto di tale motore venga effettuata a partire dal nome di una persona fisica, dal momento che detto trattamento consente a qualsiasi utente di Internet di ottenere, mediante l'elenco di risultati, una visione complessiva strutturata delle informazioni relative a questa persona reperibili su Internet, che toccano potenzialmente una moltitudine di aspetti della sua vita privata e che, senza il suddetto motore di ricerca, non avrebbero potuto – o solo difficilmente avrebbero potuto – essere connesse tra loro, e consente dunque di stabilire un profilo più o meno dettagliato di tale persona. Inoltre, l'effetto dell'ingerenza nei suddetti diritti della persona interessata risulta moltiplicato in ragione del ruolo importante che svolgono Internet e i motori di ricerca nella società moderna, i quali conferiscono alle informazioni contenute in un siffatto elenco di risultati carattere ubiquitario (v., in tal senso, sentenza *eDate Advertising e a.*, C509/09 e C161/10, EU:C:2011:685, punto 45).

81. Vista la gravità potenziale di tale ingerenza, è giocoforza constatare che quest'ultima non può essere giustificata dal semplice interesse economico del gestore di un siffatto motore di ricerca in questo trattamento di dati. Tuttavia, poiché la soppressione di link dall'elenco di risultati potrebbe, a seconda dell'informazione in questione, avere ripercussioni sul legittimo interesse degli utenti di Internet potenzialmente interessati ad avere accesso a quest'ultima, occorre ricercare, in situazioni quali quelle oggetto del procedimento principale, un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta. Se indubbiamente i diritti della persona interessata tutelati da tali articoli prevalgono, di norma, anche sul citato interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica.

82. L'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di applicazione degli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46, da effettuarsi allorché ricevono una domanda quale quella oggetto del procedimento principale, possono ordinare al suddetto gestore di sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a tale persona, senza che un'ingiunzione in tal senso presupponga che tale nome e tali informazioni siano, con il pieno consenso dell'editore o su ingiunzione di una delle autorità sopra menzionate, previamente o simultaneamente cancellati dalla pagina web sulla quale sono stati pubblicati.

83. Infatti, come si è constatato ai punti da 35 a 38 della presente sentenza, poiché il trattamento dei dati effettuato nel contesto dell'attività di un motore di ricerca si distingue da e si aggiunge a quello effettuato dagli editori di siti web e incide ulteriormente sui diritti fondamentali della persona interessata, il gestore di tale motore di ricerca quale responsabile del trattamento in questione deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che tale trattamento soddisfi le prescrizioni della direttiva 95/46, affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti.

84. In proposito occorre rilevare che, tenuto conto della facilità con cui informazioni pubblicate su un sito web possono essere riprodotte su altri siti, nonché del fatto che i responsabili della loro pubblicazione non sempre sono assoggettati alla normativa dell'Unione, non sarebbe possibile realizzare una tutela efficace e completa delle persone interessate nel caso in cui queste dovessero preventivamente o in parallelo ottenere dagli editori di siti web la cancellazione delle informazioni che le riguardano.

85. Inoltre, il trattamento da parte dell'editore di una pagina web, consistente nella pubblicazione di informazioni relative a una persona fisica, può, eventualmente, essere effettuato «esclusivamente a scopi giornalistici» e beneficiare così, a norma dell'articolo 9 della direttiva 95/46, di deroghe alle prescrizioni dettate da quest'ultima, mentre non sembra integrare tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca. Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 contro il suddetto gestore del motore di ricerca, ma non contro l'editore della pagina web.

86. Infine, occorre constatare che non soltanto il motivo giustificante, a norma dell'articolo 7 della direttiva 95/46, la pubblicazione di un dato personale su un sito web non coincide necessariamente con il motivo che si applica all'attività dei motori di ricerca,

ma che, anche quando tale coincidenza sussista, il risultato del bilanciamento degli interessi in gioco da effettuarsi ai sensi degli articoli 7, lettera f), e 14, primo comma, lettera a), di detta direttiva può divergere a seconda che si tratti del trattamento effettuato dal gestore di un motore di ricerca o di quello effettuato dall'editore di detta pagina web, in quanto, da un lato, i legittimi interessi che giustificano questi trattamenti possono essere differenti e, dall'altro, le conseguenze che tali trattamenti hanno per la persona interessata, e segnatamente per la sua vita privata, non sono necessariamente le stesse.

87. Infatti, l'inclusione nell'elenco di risultati – che appare a seguito di una ricerca effettuata a partire dal nome di una persona – di una pagina web e delle informazioni in essa contenute relative a questa persona, poiché facilita notevolmente l'accessibilità di tali informazioni a qualsiasi utente di Internet che effettui una ricerca sulla persona di cui trattasi e può svolgere un ruolo decisivo per la diffusione di dette informazioni, è idonea a costituire un'ingerenza più rilevante nel diritto fondamentale al rispetto della vita privata della persona interessata che non la pubblicazione da parte dell'editore della suddetta pagina web.

88. Alla luce dell'insieme delle considerazioni sopra esposte, occorre rispondere alla seconda questione, lettere c) e d), dichiarando che gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, al fine di rispettare i diritti previsti da tali disposizioni, e sempre che le condizioni da queste fissate siano effettivamente soddisfatte, il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita.

Sulla terza questione, concernente la portata dei diritti della persona interessata garantiti dalla direttiva 95/46

89. Con la sua terza questione, il giudice del rinvio chiede, in sostanza, se gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 debbano essere interpretati nel senso che consentono alla persona interessata di esigere dal gestore di un motore di ricerca che questi sopprima dall'elenco di risultati, che appare a seguito di una ricerca effettuata a partire dal nome di questa persona, dei link verso pagine web legittimamente pubblicate da terzi e contenenti informazioni veritiere riguardanti quest'ultima, a motivo del fatto che tali informazioni possono arrecarle pregiudizio o che essa desidera l'«oblio» di queste informazioni dopo un certo tempo.

90. Google Spain, Google Inc., i governi ellenico, austriaco e polacco, nonché la

Commissione, ritengono che tale questione esiga una risposta negativa. Google Spain, Google Inc., il governo polacco e la Commissione fanno valere in proposito che gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 conferiscono dei diritti alle persone interessate unicamente a condizione che il trattamento in parola sia incompatibile con la direttiva stessa, oppure in ragione di motivi preminenti e legittimi attinenti alla loro situazione particolare, e non per il semplice fatto che tali persone ritengano che tale trattamento possa arrecare loro pregiudizio o che esse desiderino che i dati costituenti l'oggetto di detto trattamento cadano nell'oblio. I governi ellenico e austriaco reputano che la persona interessata debba rivolgersi all'editore del sito web in questione.

91. Il sig. Costeja González nonché i governi spagnolo e italiano ritengono che la persona interessata possa opporsi all'indicizzazione dei propri dati personali ad opera di un motore di ricerca, qualora la diffusione di tali dati tramite quest'ultimo le arrechi pregiudizio e i diritti fondamentali di questa persona alla protezione dei dati suddetti e al rispetto della vita privata, comprendenti il «diritto all'oblio», prevalgano sui legittimi interessi del gestore del motore di ricerca e sull'interesse generale alla libertà d'informazione.

92. Quanto all'articolo 12, lettera b), della direttiva 95/46, la cui applicazione è subordinata alla condizione che il trattamento di dati personali sia incompatibile con la direttiva stessa, occorre ricordare che, come si è rilevato al punto 72 della presente sentenza, un'incompatibilità siffatta può derivare non soltanto dal fatto che tali dati siano inesatti, ma anche segnatamente dal fatto che essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici.

93. Da tali prescrizioni, dettate dall'articolo 6, paragrafo 1, lettere da c) a e), della direttiva 95/46, discende che anche un trattamento inizialmente lecito di dati esatti può divenire, con il tempo, incompatibile con la direttiva suddetta qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura in particolare nel caso in cui i dati risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso.

94. Pertanto, nell'ipotesi in cui si constati, in seguito a una domanda della persona interessata ai sensi dell'articolo 12, lettera b), della direttiva 95/46, che l'inclusione nell'elenco di risultati – che appare a seguito di una ricerca effettuata a partire dal suo nome – dei link verso pagine web, legittimamente pubblicate da terzi e contenenti informazioni veritiere relative alla sua persona, è, allo stato attuale, incompatibile con il citato articolo 6, paragrafo 1, lettere da c) a e), a motivo del fatto che tali informazioni appaiono, alla

luce dell'insieme delle circostanze caratterizzanti il caso di specie, inadeguate, non pertinenti o non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento in questione realizzato dal gestore del motore di ricerca, le informazioni e i link in parola di cui al suddetto elenco di risultati devono essere cancellati.

95. Per quanto riguarda le domande ai sensi del suddetto articolo 12, lettera b), fondate sul presunto mancato rispetto delle condizioni previste dall'articolo 7, lettera f), della direttiva 95/46, nonché le domande a norma dell'articolo 14, primo comma, lettera a), della medesima direttiva, occorre rilevare che ciascun trattamento di dati personali deve essere legittimato in virtù di tale articolo 7 per tutto il tempo in cui viene effettuato.

96. Alla luce di quanto precede, nel valutare domande di questo tipo proposte contro un trattamento di dati quale quello in esame nel procedimento principale, occorre verificare in particolare se l'interessato abbia diritto a che l'informazione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome. In proposito occorre sottolineare che la constatazione di un diritto siffatto non presuppone che l'inclusione dell'informazione in questione nell'elenco di risultati arrechi un pregiudizio all'interessato.

97. Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico mediante la sua inclusione in un siffatto elenco di risultati, occorre considerare – come risulta in particolare dal punto 81 della presente sentenza – che i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi.

98. Relativamente ad una situazione come quella in esame nel procedimento principale, che riguarda la visualizzazione – nell'elenco di risultati che l'utente di Internet ottiene effettuando una ricerca a partire dal nome della persona interessata con l'aiuto di Google Search – di link verso pagine degli archivi online di un quotidiano, contenenti annunci che menzionano il nome di tale persona e si riferiscono ad un'asta immobiliare legata ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali, occorre affermare che, tenuto conto del carattere sensibile delle informazioni contenute in tali annunci per la vita privata di detta persona, nonché del fatto che la loro pubbli-

cazione iniziale era stata effettuata 16 anni prima, la persona interessata vanta un diritto a che tali informazioni non siano più collegate al suo nome attraverso un elenco siffatto. Pertanto, dal momento che nella fattispecie non sembrano sussistere ragioni particolari giustificanti un interesse preponderante del pubblico ad avere accesso, nel contesto di una ricerca siffatta, a dette informazioni – aspetto questo che spetta però al giudice del rinvio verificare –, la persona interessata può esigere, a norma degli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46, la soppressione dei link suddetti da tale elenco di risultati.

99. Dalle suesposte considerazioni discende che occorre rispondere alla terza questione dichiarando che gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato. Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi.

Sulle spese

100. Nei confronti delle parti nella causa principale il presente procedimento costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) L'articolo 2, lettere b) e d), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, deve essere

interpretato nel senso che, da un lato, l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come «trattamento di dati personali», ai sensi del citato articolo 2, lettera b), qualora tali informazioni contengano dati personali, e che, dall'altro lato, il gestore di detto motore di ricerca deve essere considerato come il «responsabile» del trattamento summenzionato, ai sensi dell'articolo 2, lettera d), di cui sopra.

2) L'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro.

3) Gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, al fine di rispettare i diritti previsti da tali disposizioni, e sempre che le condizioni da queste fissate siano effettivamente soddisfatte, il gestore di un motore di ricerca è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, dei link verso pagine web pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine web di cui trattasi, e ciò eventualmente anche quando la loro pubblicazione su tali pagine web sia di per sé lecita.

4) Gli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 devono essere interpretati nel senso che, nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato. Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico in virtù della sua inclusione in un siffatto elenco di risultati, i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concer-

nente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi.

2.

CONCLUSIONI DELL'AVVOCATO GENERALE Niilo JÄÄSKINEN

presentate il 25 giugno 2013 nella causa C131/12¹

Google Spain SL

Google Inc.

contro

Agencia Española de Protección de Datos (AEPD)

Mario Costeja González

[domanda di pronuncia pregiudiziale proposta dalla Audiencia Nacional (Spagna)]

I –INTRODUZIONE

1. Nel 1890, nel loro storico articolo sulla *Harvard Law Review* intitolato «The Right to Privacy»², Samuel D. Warren e Louis D. Brandeis denunciavano che «[i]nvenzioni e tecniche commerciali recenti», come «le fotografie e i giornali [, avevano] invaso i sacri recinti della vita privata e domestica». In quello stesso articolo i due autori facevano riferimento ai «passi da intraprendere per la tutela della persona».

2. Al giorno d'oggi, la protezione dei dati personali e della vita privata degli individui è divenuta sempre più importante. Qualsiasi tipo di contenuto che comprenda dati personali, che si tratti di testi o di materiali audiovisivi, può essere reso accessibile, all'istante e in maniera permanente, in formato digitale in tutto il mondo. Internet ha rivoluzionato le nostre vite rimuovendo le barriere tecniche e istituzionali alla diffusione e alla ricezione delle informazioni ed ha creato una piattaforma per numerosi servizi della società dell'informazione. Tali servizi vanno a beneficio dei consumatori, delle imprese e della società in generale. Ciò ha dato origine a situazioni senza precedenti, nelle quali occorre trovare un equilibrio tra più diritti fondamentali, come la libertà di espressione, la libertà di informazione e la libertà di impresa, da un lato, e la tutela dei dati personali e della riservatezza degli individui, dall'altro lato.

¹ Lingua originale: l'inglese.

² *Harvard Law Review*, vol. IV, n. 5, del 15 dicembre 1890.

3. Per quanto riguarda Internet, vanno distinte tre situazioni relative ai dati personali. La prima è la pubblicazione di dati personali su una qualsiasi pagina web di Internet³ (la «pagina web source»)⁴ La seconda riguarda il caso in cui un motore di ricerca su Internet fornisca risultati di ricerca che indirizzano l'utente di Internet verso la pagina web source. La terza situazione, meno evidente, ricorre quando un utente di Internet effettua una ricerca utilizzando un motore di ricerca su Internet e alcuni dei suoi dati personali, come l'indirizzo IP dal quale la ricerca viene effettuata, vengono automaticamente trasferiti al fornitore di servizi di motore di ricerca su Internet⁵.

4. Per quanto riguarda la prima situazione, nella sentenza Lindqvist la Corte ha già dichiarato che le è applicabile la direttiva 95/46/CE⁶) (in prosieguo: la «direttiva sulla

³ Di fatto, «Internet» comprende due servizi principali, ossia il World Wide Web e i servizi di posta elettronica. Sebbene Internet, in quanto rete di computer interconnessi, esista da un certo tempo sotto diverse forme, a cominciare da Arpanet (Stati Uniti), la rete aperta e liberamente accessibile con indirizzi www e una struttura comune dei codici è iniziata soltanto al principio degli anni '90. A quanto risulta, il termine storicamente corretto sarebbe World Wide Web. Tuttavia, tenuto conto dell'uso corrente e delle scelte terminologiche effettuate nella giurisprudenza della Corte, qui di seguito verrà principalmente utilizzato il termine «Internet» con riferimento alla parte World Wide Web della rete.

⁴ – La collocazione delle pagine web è identificata con un indirizzo individuale, l'URL (Uniform Resource Locator), un sistema creato nel 1994. Si può accedere ad una pagina web digitando il suo URL nel web browser [navigatore web], direttamente o con l'aiuto di un nome di dominio. Le pagine web devono essere codificate con un linguaggio di marcatura. L'HyperText Markup Language (HTML) è il principale linguaggio di marcatura per la creazione di pagine web e di altre informazioni visualizzabili in un web browser.

⁵ La portata delle tre questioni è illustrata dalle informazioni seguenti (anche se non sono disponibili dati precisi). In primo luogo, è stato stimato che esistano oltre 600 milioni di siti web in Internet. In questi siti Internet vi sarebbero oltre 40 miliardi di pagine web. In secondo luogo, riguardo ai motori di ricerca, il loro numero è molto più limitato: esisterebbero meno di 100 motori di ricerca importanti e attualmente Google deterrebbe una quota enorme su molti mercati. È stato detto che il successo del motore di ricerca di Google è basato su web crawler [programmi per la raccolta di informazioni o programmi spider] estremamente potenti, su sistemi di indicizzazione efficaci e su una tecnologia che consente di classificare i risultati della ricerca in base alla loro rilevanza per l'utente (compreso l'algoritmo brevettato PageRank): v. LópezTarruella, A., «Introduction: Google Pushing the Boundaries of Law», *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge Economy Business Models*, ed. LópezTarruella, A., T.M.C., Asser Press, L'Aja, 2012, pp. da 1 a 8, in particolare p. 2. In terzo luogo, oltre tre quarti degli Europei utilizzano Internet e, nella misura in cui essi utilizzano motori di ricerca, i loro dati personali, in quanto utenti di motori di ricerca su Internet, possono essere raccolti e trattati dal motore di ricerca su Internet di cui si sono serviti.

⁶ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché

protezione dei dati personali» o la «direttiva»). La terza situazione non è oggetto di discussione nella presente causa e sono in corso procedimenti amministrativi promossi da autorità nazionali competenti per la protezione dei dati allo scopo di chiarire agli utenti di motori di ricerca su Internet l'ambito di applicazione delle norme dell'Unione in materia di protezione dei dati⁷.

5. L'ordinanza di rinvio nella presente causa riguarda la seconda situazione. Essa è stata formulata dall'Audiencia Nacional (Corte suprema, Spagna) nell'ambito di una controversia tra Google Spain SL e Google Inc. (in prosieguo, individualmente o congiuntamente: «Google»), da un lato, e l'Agencia Española de Protección de Datos (in prosieguo: l'«AEPD») e il signor Mario Costeja González (in prosieguo: la «persona interessata» o l'«interessato»), dall'altro lato. Il procedimento verte sull'applicazione della direttiva sulla protezione dei dati personali ad un motore di ricerca su Internet che Google gestisce come fornitore di servizi. Nel procedimento nazionale è assodato che alcuni dati personali relativi alla persona interessata sono stati pubblicati da un giornale spagnolo in due delle sue edizioni cartacee nel 1998, entrambe ripubblicate successivamente in versione elettronica disponibile su Internet. La persona interessata ritiene oggi che tali informazioni non dovrebbero più essere visualizzate nei risultati di ricerca presentati dal motore di ricerca su Internet gestito da Google nel momento in cui viene effettuata una ricerca del suo nome e cognome.

6. Le questioni deferite alla Corte si suddividono in tre gruppi⁸. Il primo gruppo di quesiti [la prima questione] si riferisce all'*ambito territoriale di applicazione* delle norme dell'Unione sulla protezione dei dati. Il secondo gruppo [la seconda questione] tratta della posizione giuridica di un fornitore di servizi di motore di ricerca su Internet⁹ alla luce

alla libera circolazione di tali dati (GU L 281, p. 31).

⁷ V., in generale, Gruppo di lavoro Articolo 29 per la protezione dei dati personali, parere n. 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca (WP 148). La politica di riservatezza seguita da Google riguardo agli utenti del suo motore di ricerca viene esaminata dalle autorità degli Stati membri incaricate della protezione dei dati personali. L'azione è condotta dall'Autorità francese per la tutela dei dati personali (la CNIL). Per sviluppi recenti, v. la lettera del 16 ottobre 2012 inviata a Google dal Gruppo di lavoro Articolo 29, disponibile sul sito Internet menzionato alla nota 22.

⁸ V. infra, paragrafo 19.

⁹ Nel prosieguo, con l'espressione «motore di ricerca su Internet» si farà riferimento alla combinazione di software e strumenti che rende possibile la ricerca di testi e contenuti audiovisivi su Internet. Le questioni specifiche relative ai motori di ricerca operanti all'interno di un dominio Internet definito (o sito web), come <http://curia.europa.eu>, non sono oggetto di discussione nelle presenti conclusioni. L'operatore economico che fornisce l'accesso ad un motore di ricerca verrà definito con l'espressione «fornitore di servizi di motore di ricerca su Internet». Nella presente causa, è Google Inc. il fornitore di servizi che danno accesso al motore di ricerca Google nonché a numerose altre funzioni

della direttiva, segnatamente in relazione al suo *ambito di applicazione ratione materiae*. Infine, la terza questione verte sul cosiddetto *diritto all'oblio* e sulla questione se le persone interessate possano chiedere che tutti o parte dei risultati di ricerca che le riguardano non siano più accessibili attraverso il motore di ricerca. Tutti i suddetti quesiti, che sollevano anche problemi importanti relativi alla tutela dei diritti fondamentali, sono una novità per la Corte.

7. Questa sarebbe la prima causa in cui la Corte è chiamata ad interpretare la direttiva con riferimento ai motori di ricerca su Internet; una questione, a quanto pare, di attualità per le autorità nazionali competenti per la protezione dei dati e per i giudici degli Stati membri. Difatti, il giudice di rinvio ha dichiarato di essere investito di molte cause analoghe.

8. Il più importante precedente sottoposto alla Corte nel quale sono stati affrontati problemi relativi alla protezione dei dati e a Internet è la controversia che ha dato luogo alla sentenza Lindqvist¹⁰. Tale causa, però, non verteva sui motori di ricerca su Internet. La direttiva stessa è stata oggetto di interpretazione in una serie di cause. Tra queste, le cause Österreichischer Rundfunk e a.¹¹, Satakunnan Markkinapörssi e Satamedia¹² e Volker und Markus Schecke e Eifert¹³ sono particolarmente importanti. Inoltre, il ruolo dei motori di ricerca su Internet in relazione ai diritti di proprietà intellettuale e alla competenza giurisdizionale sono stati esaminati dalla Corte nelle cause Google France e Google, Portakabin, L'Oréal e a., Interflora e Interflora British Unit, e Wintersteiger¹⁴.

9. Dopo l'adozione della direttiva, una disposizione sulla protezione dei dati personali è stata inserita nell'articolo 16 TFUE e nell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»). Inoltre, nel 2012 la Commissione ha presentato una proposta di regolamento generale sulla protezione dei dati¹⁵ da sostituire alla direttiva. La presente causa, tuttavia, dev'essere decisa sulla base del diritto vigente.

10. La domanda pregiudiziale in esame è caratterizzata dal fatto che, nel momento

di ricerca, come maps.google.com e news.google.com.

¹⁰ Sentenza del 6 novembre 2003 (C101/01, Racc. p. I12971).

¹¹ Sentenza del 20 maggio 2003 (C465/00, C138/01 e C139/01, Racc. p. I4989).

¹² Sentenza del 16 dicembre 2008 (C73/07, Racc. p. I9831).

¹³ Sentenza del 9 novembre 2010 (C92/09 e C93/09, Racc. p. I11063).

¹⁴ Sentenze, rispettivamente, del 23 marzo 2010 (da C236/08 a C238/08, Racc. p. I2417); dell'8 luglio 2010 (C558/08, Racc. p. I6963); del 12 luglio 2011 (C324/09, Racc. p. I6011); del 22 settembre 2011 (C323/09, Racc. p. I8625) e del 19 aprile 2012 (C523/10, non ancora pubblicata nella Raccolta).

¹⁵ Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012) 11 def.

in cui è stata elaborata la proposta di direttiva della Commissione nel 1990, Internet nell'attuale significato del World Wide Web non esisteva né esistevano motori di ricerca. All'epoca in cui la direttiva è stata adottata, nel 1995, Internet era appena stato lanciato e cominciavano ad apparire i primi rudimentali motori di ricerca, ma nessuno avrebbe potuto prevedere quanto profondamente tutto questo avrebbe cambiato il mondo. Oggigiorno praticamente chiunque possieda uno smartphone o un computer può essere considerato svolgere attività su Internet alle quali sarebbe applicabile la direttiva.

II – CONTESTO NORMATIVO

A – La direttiva sulla protezione dei dati personali

11. Ai sensi dell'articolo 1 della direttiva, gli Stati membri garantiscono, conformemente alle disposizioni della direttiva stessa, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

12. L'articolo 2 definisce, tra le altre, la nozione di «dati personali» e di «persona interessata», di «trattamento di dati personali», di «responsabile del trattamento» e di «terzi».

13. Ai sensi dell'articolo 3, le disposizioni della direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché, in certe situazioni, al trattamento non automatizzato.

14. Ai sensi dell'articolo 4, paragrafo 1, gli Stati membri applicano le disposizioni nazionali adottate per l'attuazione della direttiva al trattamento di dati personali effettuato là dove vi sia uno stabilimento del responsabile del trattamento nel loro territorio o, se il responsabile non è stabilito nell'Unione, nei casi in cui egli ricorra, ai fini del trattamento di dati personali, a strumenti situati nel territorio degli Stati membri.

15. L'articolo 12 della direttiva attribuisce alle persone interessate un «diritto di accesso» ai dati personali trattati dal responsabile del trattamento e l'articolo 14 un «diritto di opporsi» al trattamento di tali dati in alcune situazioni.

16. L'articolo 29 della direttiva istituisce un Gruppo di lavoro consultivo indipendente composto, inter alia, da autorità degli Stati membri per la protezione dei dati (in prosieguo: il «Gruppo di lavoro Articolo 29»).

B – Diritto nazionale

17. La legge organica n. 15/1999 sulla protezione dei dati ha trasposto la direttiva

nel diritto spagnolo¹⁶.

III – FATTI E QUESTIONI PREGIUDIZIALI

18. Agli inizi del 1998, un giornale di ampia diffusione in Spagna pubblicava nella sua edizione cartacea due annunci relativi ad un'asta di beni immobili collegata ad un procedimento esecutivo derivante da debiti contratti con il sistema previdenziale. La persona interessata era menzionata come proprietario degli immobili. Successivamente, l'editore rendeva disponibile online una versione elettronica del giornale.

19. Nel novembre 2009 la persona interessata contattava l'editore del giornale facendo valere che, inserendo il suo nome e cognome nel motore di ricerca Google, compariva un riferimento che rinviava alle pagine del giornale contenenti gli annunci relativi all'asta immobiliare. Egli affermava che il procedimento esecutivo per debiti con il sistema previdenziale si era concluso e risolto da vari anni e che attualmente era irrilevante. L'editore ribatteva che non era appropriato eliminare i dati che riguardavano l'interessato, in quanto la pubblicazione era stata fatta per ordine del Ministero del Lavoro e della Previdenza sociale.

20. Nel febbraio 2010 la persona interessata contattava Google Spain e chiedeva che, in caso di inserimento del suo nome e cognome nel motore di ricerca Google, i risultati della ricerca non mostrassero più i link verso il giornale. Google Spain inoltrava la richiesta a Google Inc., la cui sede sociale è in California (Stati Uniti), considerando che fosse quest'ultima l'impresa fornitrice del servizio di ricerca Internet.

21. Successivamente, la persona interessata presentava reclamo dinanzi all'AEPD chiedendo di ordinare all'editore la rimozione o la modifica dell'informazione pubblicata, in modo che non comparissero più i suoi dati personali, oppure di utilizzare gli strumenti forniti dai motori di ricerca per tutelare i suoi dati personali. Egli chiedeva inoltre di ordinare a Google Spain o a Google Inc. di eliminare o occultare i suoi dati, in modo che non comparissero più tra i risultati della ricerca né mostrassero più links al quotidiano.

22. Con decisione del 30 luglio 2010, il direttore dell'AEPD accoglieva il reclamo della persona interessata nei confronti di Google Spain e di Google Inc., invitando tali imprese ad adottare le misure necessarie per ritirare i dati dal loro indice e impedire l'accesso futuro ai medesimi, ma respingeva il reclamo nei confronti dell'editore. La motivazione era che la pubblicazione dei dati sulla stampa era legalmente giustificata. Google Spain e Google Inc. hanno proposto ciascuna impugnazione dinanzi al giudice del rinvio, chiedendo l'annullamento della decisione dell'AEPD.

¹⁶ BOE n. 298, del 14 dicembre 1999, p. 43088.

23. Il giudice nazionale ha sospeso il procedimento e sottoposto alla Corte le seguenti questioni pregiudiziali:

«1. Per quanto concerne l'ambito territoriale di applicazione della [direttiva] e, di conseguenza, della normativa spagnola sulla protezione dei dati:

1.1. se debba ritenersi che esiste uno “stabilimento” ai sensi dell'articolo 4, paragrafo 1, lettera a), della [direttiva], qualora ricorrano una o più delle seguenti circostanze:

- l'impresa che gestisce il motore di ricerca apre in uno Stato membro un'agenzia o una filiale, con l'incarico di promuovere e di vendere gli spazi pubblicitari del motore di ricerca, la quale dirige la propria attività agli abitanti di tale Stato;
- la società madre designa una filiale stabilita in tale Stato membro come suo rappresentante e responsabile del trattamento di due file specifici contenenti i dati dei clienti che hanno contrattato con tale società per la fornitura di servizi pubblicitari;
- l'agenzia o la filiale stabilita in uno Stato membro trasmette alla società madre avente sede al di fuori dell'Unione europea i reclami e le ingiunzioni che le sono inoltrati tanto dalle persone interessate quanto dalle autorità competenti perché sia rispettato il diritto alla protezione dei dati, anche quando tale collaborazione abbia carattere volontario.

1.2. Se l'articolo 4, paragrafo 1, lettera c), della [direttiva] debba essere interpretato nel senso che si configura un ricorso “a strumenti situati nel territorio di detto Stato membro” qualora un motore di ricerca:

- utilizzi uno spider o un robot per localizzare e indicizzare le informazioni contenute nelle pagine web alloggiate sui server di tale Stato membro

o

- utilizzi un nome di dominio di uno Stato membro e indirizzi le ricerche e i risultati in funzione della lingua di tale Stato membro.

1.3. Se possa considerarsi un ricorso a strumenti ai sensi dell'articolo 4, paragrafo 1, lettera c), della [direttiva] la memorizzazione temporanea delle informazioni indicizzate dai motori di ricerca su Internet. In caso di risposta affermativa a quest'ultimo quesito, se si possa ritenere soddisfatto tale criterio di collegamento quando, per ragioni di concorrenza, la società rifiuta di rivelare il luogo in cui archivia i detti indici.

1.4. A prescindere dalla risposta ai precedenti quesiti, e specialmente nel caso in cui la [Corte] ritenesse inapplicabili i criteri di collegamento previsti all'articolo 4 della direttiva

va, se, alla luce dell'articolo 8 della [Carta], la [direttiva] debba essere applicata nello Stato membro dove si trova il centro di gravità del conflitto e sia possibile ottenere una tutela più efficace dei diritti dei cittadini dell'Unione europea.

2. Per quanto riguarda l'attività dei motori di ricerca quali fornitori di contenuti in relazione alla [direttiva]:

2.1. quanto all'attività del motore di ricerca su Internet della società Google, quale fornitore di contenuti, consistente nel localizzare le informazioni pubblicate o messe in rete da terzi, indicizzarle in maniera automatica, memorizzarle temporaneamente e infine metterle a disposizione degli internauti secondo un determinato ordine di preferenza, qualora tali informazioni contengano dati personali di terzi,

se un'attività come quella descritta debba essere considerata rientrare nella nozione di "trattamento di dati" ai sensi dell'articolo 2, lettera b), della [direttiva].

2.2. In caso di risposta affermativa al quesito sub 2.1, e sempre con riferimento ad un'attività come quella descritta, se l'articolo 2, lettera d), della [direttiva] debba essere interpretato nel senso che la società che gestisce il motore di ricerca Google deve essere considerata "responsabile del trattamento" dei dati personali contenuti nelle pagine web da essa indicizzate.

2.3. In caso di risposta affermativa al quesito sub 2.2, se l'autorità nazionale di controllo dei dati (nel caso presente l'[AEPD]), al fine di tutelare i diritti enunciati agli articoli 12, lettera b), e 14), lettera a), della [direttiva], possa ordinare direttamente al motore di ricerca della società Google di ritirare dai suoi indici un'informazione pubblicata da terzi, senza rivolgersi previamente o simultaneamente al titolare della pagina web in cui è inserita tale informazione.

2.4. In caso di risposta affermativa al quesito sub 2.3, se i motori di ricerca siano sollevati dall'obbligo di rispettare tali diritti qualora l'informazione contenente i dati personali sia stata lecitamente pubblicata da terzi e rimanga sulla pagina web di origine.

3. Rispetto alla portata del diritto alla cancellazione/opposizione al trattamento dati in relazione al "diritto di oblio", si pone la seguente questione:

3.1. se si debba ritenere che i diritti di cancellazione e congelamento dei dati, disciplinati dall'articolo 12, lettera b), e il diritto di opposizione al loro trattamento, regolato dall'articolo 14, lettera a), della [direttiva], implicino che l'interessato possa rivolgersi ai motori di ricerca per impedire l'indicizzazione delle informazioni riguardanti la sua persona, pubblicate sulla pagina web di terzi, facendo valere la propria volontà che tali

informazioni non siano divulgate agli utenti di Internet, ove reputi che detta divulgazione possa nuocergli o desideri che tali informazioni siano dimenticate, sebbene si tratti di informazioni pubblicate da terzi lecitamente».

24. Osservazioni scritte sono state presentate da Google, dai governi di Spagna, Grecia, Italia, Austria e Polonia nonché dalla Commissione europea. Tranne il governo polacco, tutti, compresa la persona interessata, hanno preso parte all'udienza del 26 febbraio 2013 ed hanno presentato osservazioni orali.

IV – OSSERVAZIONI PRELIMINARI

A – Rilievi introduttivi

25. Il problema principale di cui alla presente causa è sapere come debba essere interpretato il ruolo svolto dai fornitori di servizi di motore di ricerca su Internet alla luce dei vigenti strumenti giuridici dell'Unione in materia di protezione dei dati, in particolare alla luce della direttiva. È pertanto utile iniziare con alcune osservazioni riguardanti lo sviluppo della protezione dei dati, Internet e i motori di ricerca su Internet.

26. Quando la direttiva è stata negoziata e adottata nel 1995¹⁷, le è stato attribuito un ampio ambito di applicazione *ratione materiae*. Ciò perché gli sviluppi tecnologici avevano consentito ai responsabili del trattamento di dati un trattamento maggiormente decentrato rispetto ai sistemi di archiviazione basati sulle tradizionali banche dati centralizzate, che comprendeva altresì nuovi tipi di dati personali, come le immagini, e di tecniche di trattamento, come le ricerche testuali libere¹⁸.

27. Nel 1995, l'accesso generalizzato a Internet era un fenomeno nuovo. Oggi, a distanza di quasi due decenni, il volume dei contenuti digitali disponibili online è esplosivo. È possibile accedervi facilmente, consultarli e diffonderli tramite i social media, così come scaricarli su diversi apparecchi, come tablet, smartphone e computer portatili. Tuttavia, è evidente che il legislatore comunitario non aveva previsto che Internet si sarebbe evoluto in un deposito completo e globale di informazioni, accessibile e consultabile dappertutto.

28. Al centro del presente rinvio pregiudiziale è il fatto che Internet amplifica e faci-

¹⁷ Ai sensi del considerando 11, i «principi della tutela dei diritti e delle libertà delle persone, in particolare del rispetto della vita privata, contenuti dalla presente direttiva precisano ed ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale».

¹⁸ Gruppo di lavoro Articolo 29, parere n. 1/2010 sui concetti di «responsabile del trattamento» e «incaricato del trattamento» (WP 169), pp. 3 e 4.

lita in modo inedito la diffusione di informazioni¹⁹. Come l'invenzione della stampa nel XV secolo ha consentito di riprodurre un numero illimitato di copie che prima dovevano essere scritte a mano, così caricare materiali su Internet permette un accesso di massa a informazioni che prima potevano essere reperite solo dopo faticose ricerche e in posti fisicamente limitati. L'accesso universale all'informazione online è possibile ovunque, con l'eccezione di quei paesi le cui autorità hanno limitato l'accesso a Internet con diversi mezzi tecnici (come i firewall elettronici) o nei quali l'accesso alle telecomunicazioni è controllato o scarso.

29. A causa di queste evoluzioni, l'ambito di applicazione potenziale della direttiva nel mondo moderno è divenuto sorprendentemente ampio. Si pensi ad un professore di diritto europeo che abbia scaricato sul suo portatile la giurisprudenza essenziale della Corte dal sito della stessa. A termini della direttiva, questo professore potrebbe essere considerato un «responsabile del trattamento» di dati personali provenienti da un soggetto terzo. Il professore è in possesso di file contenenti dati personali trattati automaticamente a scopo di ricerca e di consultazione nell'ambito di attività che non sono puramente personali o domestiche. In realtà, chiunque oggi legga un giornale su un tablet o segua un social media su uno smartphone apparentemente effettua un trattamento di dati personali tramite strumenti automatizzati e potrebbe teoricamente rientrare nell'ambito di applicazione della direttiva nella misura in cui tale attività si svolga al di fuori della sua stretta sfera privata²⁰. Per di più, l'ampia interpretazione che la Corte ha dato del diritto fondamentale alla vita privata nell'ambito della protezione dei dati personali sembra esporre qualunque comunicazione umana effettuata tramite mezzi elettronici ad essere esaminata alla luce di tale diritto.

30. Nella situazione attuale, le ampie definizioni delle nozioni di dati personali, trattamento dei dati personali e responsabile del trattamento sono atte a coprire una serie mai così ampia di nuove situazioni di fatto legate all'evoluzione tecnologica. Ciò è dovuto alla circostanza che la maggior parte, se non la totalità, dei siti Internet e dei file accessibili loro tramite contengono dati personali, come i nomi di persone fisiche viventi. Questo impone alla Corte di applicare una regola di ragionevolezza, ossia il principio di

¹⁹ Per esempio, sentenza del 25 ottobre 2011, *eDate Advertising e Martinez* (C509/09 e C161/10, Racc. p. I10269, punto 45).

²⁰ Di solito un giornale contiene dati personali, come i nomi di persone fisiche. Questi dati personali sono trattati nel momento in cui vengono consultati tramite mezzi automatizzati. Tale trattamento ricade nell'ambito di applicazione della direttiva, a meno che non sia effettuato da una persona fisica nell'esercizio di attività puramente personali o domestiche. V. articolo 2, lettere a) e b), e articolo 3, paragrafo 2, della direttiva. Inoltre, anche la lettura di un documento cartaceo o la visualizzazione di immagini contenenti dati personali equivale a un trattamento degli stessi. V. Dammann, U., e Simitis, S., *EG-Datenschutzrichtlinie*, Nomos Verlagsgesellschaft, Baden-Baden, 1997, p. 110.

proporzionalità, nell'interpretare l'ambito della direttiva, al fine di evitare conseguenze giuridiche irrazionali ed eccessive. La Corte ha già seguito questo approccio moderato nella sentenza Lindqvist, nella quale ha respinto un'interpretazione che avrebbe potuto portare ad attribuire un ambito di applicazione di ampiezza ingiustificata all'articolo 25 della direttiva, relativo al trasferimento di dati personali verso paesi terzi nell'ambito di Internet²¹.

31. Pertanto, nella presente causa bisognerà trovare un equilibrio corretto, ragionevole e proporzionato tra la protezione dei dati personali, l'interpretazione coerente degli obiettivi della società dell'informazione e gli interessi legittimi degli operatori economici e degli utenti di Internet in senso ampio. Sebbene la direttiva non abbia subito modifiche da quando è stata adottata nel 1995, la sua applicazione a situazioni nuove è stata inevitabile. Si tratta di un campo complesso in cui si confrontano il diritto e le nuove tecnologie. I pareri del Gruppo di lavoro Articolo 29 forniscono, al riguardo, analisi di grande utilità²².

B – I motori di ricerca su Internet e la protezione dei dati personali

32. Nell'analisi della posizione giuridica di un motore di ricerca su Internet alla luce delle norme sulla tutela dei dati personali è necessario porre in evidenza i seguenti elementi²³.

33. In primo luogo, nella sua forma di base, un motore di ricerca su Internet non crea, in linea di principio, contenuti autonomi nuovi. Nella sua forma più semplice, esso si limita a indicare dove può essere reperito un contenuto già esistente, messo a disposizione da terzi su Internet, fornendo un hyperlink verso il sito web contenente i termini di ricerca.

34. In secondo luogo, i risultati visualizzati da un motore di ricerca su Internet non sono basati su una ricerca istantanea dell'intero World Wide Web, ma sono raccolti dal contenuto che il motore di ricerca su Internet ha precedentemente trattato. Questo significa che il motore di ricerca su Internet ha recuperato contenuti dai siti web esistenti ed ha copiato, analizzato e indicizzato tali contenuti sui propri dispositivi. Questi contenuti recuperati includono dati personali se le pagine web source ne contengono a loro volta.

²¹ V. sentenza Lindqvist, cit., punti da 67 a 70, relativamente all'interpretazione dell'articolo 25 della direttiva.

²² I pareri sono disponibili sul sito Internet http://ec.europa.eu/justice/data-protection/index_en.htm.

²³ I motori di ricerca su Internet sono in costante evoluzione e in questa sede si intende solo dare un'idea generale delle caratteristiche essenziali attualmente rilevanti.

35. In terzo luogo, per consentire un utilizzo più funzionale dei risultati di ricerca, i motori di ricerca su Internet visualizzano spesso contenuti addizionali a fianco del link verso il sito web originale. Può trattarsi di estratti di testi, di audiovisivi o di istantanee di pagine web source. Queste anteprime di informazione possono essere, almeno in parte, recuperate dai dispositivi del fornitore di servizi di motore di ricerca su Internet e non estratte istantaneamente dal sito web originale. Di conseguenza, il fornitore di servizi detiene effettivamente le informazioni così visualizzate.

C – Regolamentazione dei motori di ricerca su Internet

36. L'Unione europea ha attribuito grande importanza allo sviluppo della società dell'informazione. In tale ambito, è stato trattato anche il ruolo degli intermediari della società dell'informazione. Questi intermediari assicurano un collegamento tra i fornitori di contenuti e gli utenti di Internet. La specificità del loro ruolo è stata riconosciuta, per esempio, nella direttiva sulla protezione dei dati personali (considerando 47), nella direttiva 2000/31 sul commercio elettronico²⁴ (articolo 21, paragrafo 2, e considerando 18) nonché nel parere n. 1/2008 del Gruppo di lavoro Articolo 29. Il ruolo dei fornitori di accesso a Internet è stato ritenuto fondamentale per la società dell'informazione e la loro responsabilità per i contenuti di terzi da essi trasferiti e/o immagazzinati è stata limitata per agevolarne le attività legittime.

37. Il ruolo e la posizione giuridica dei fornitori di servizi di motore di ricerca su Internet non sono stati oggetto di regolamentazione specifica nel diritto dell'Unione. In quanto tali, i «servizi di motori di ricerca» sono prestati a distanza, per via elettronica e su richiesta individuale di un destinatario di servizi, e corrispondono quindi ad un servizio della società dell'informazione consistente nel fornire strumenti per la ricerca, l'accesso e il reperimento di dati. Tuttavia, i fornitori di servizi di motore di ricerca su Internet come Google, i quali non prestano un servizio retribuito dagli utenti di Internet, non rientrerebbero, in questa loro qualità, nell'ambito di applicazione della direttiva 2000/31 sul commercio elettronico²⁵.

38. Malgrado ciò, è necessario esaminare la posizione alla luce dei principi giuridi-

²⁴ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («direttiva sul commercio elettronico») (GU L 178, p. 1).

²⁵ V. considerando 18 e articolo 2, lettera a), della direttiva 2000/31 sul commercio elettronico, in combinato disposto con la direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 204, p. 37), come modificata dalla direttiva 98/48 del Parlamento europeo e del Consiglio, del 20 luglio 1998 (GU L 217, p. 18).

ci che stanno alla base delle limitazioni di responsabilità dei fornitori di accesso a Internet. In altri termini, in quale misura le attività svolte da un fornitore di servizi di motore di ricerca su Internet siano analoghe, sotto il profilo dei principi sulla responsabilità, ai servizi elencati nella direttiva 2000/31 sul commercio elettronico [trasporto, semplice memorizzazione temporanea («caching»), stoccaggio («hosting»)] o ai servizi di trasmissione menzionati nel considerando 47 della direttiva, e in quale misura il fornitore di servizi di motore di ricerca su Internet agisca come fornitore autonomo di contenuto.

D – Il ruolo e la responsabilità degli editori di pagine web source

39. Nella sentenza Lindqvist la Corte ha dichiarato che «l'operazione consistente nel far comparire in una pagina Internet dati personali va considerata come un trattamento [di dati personali]»²⁶. Inoltre, «far apparire delle informazioni in una pagina Internet impone, secondo i procedimenti tecnici e informatici attualmente applicati, di realizzare un'operazione di caricamento di questa pagina su un server nonché le operazioni necessarie per rendere questa pagina accessibile a coloro che si sono collegati ad Internet. Tali operazioni vengono effettuate, almeno in parte, in modo automatizzato». La Corte ha concluso che «l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi» «costituisce un "trattamento di dati personali interamente o parzialmente automatizzato" ai sensi dell'articolo 3, paragrafo 1, della [direttiva]».

40. Dalle citate affermazioni contenute nella sentenza Lindqvist emerge che l'editore di pagine web source contenenti dati personali è un responsabile del trattamento di dati personali ai sensi della direttiva. In quanto tale, l'editore è vincolato dalla serie di obblighi che la direttiva impone ai responsabili del trattamento.

41. Le pagine web source vengono conservate su server «host» connessi a Internet. L'editore di pagine web source può avvalersi di «codici di esclusione»²⁷ per il funzionamento dei motori di ricerca su Internet. I codici di esclusione avvisano i motori di ricerca di non indicizzare o archiviare una pagina web source o di non visualizzarla nei risultati di ricerca²⁸. Il loro utilizzo indica che l'editore non vuole che certe informazioni sulle pagine web source vengano reperite per essere diffuse attraverso i motori di ricerca.

²⁶ Cit., punti da 25 a 27.

²⁷ Un tipico codice di esclusione attuale (o protocollo robot di esclusione) è chiamato «robots.txt»; v. <http://en.wikipedia.org/wiki/Robots.txt> o <http://www.robotstxt.org>.

²⁸ I codici di esclusione, tuttavia, non impediscono tecnicamente l'indicizzazione o la visualizzazione, il fornitore di servizi che gestisce un motore di ricerca può decidere di ignorarli. I principali fornitori di servizi di motore di ricerca su Internet, Google compresa, sostengono di rispettare i codici contenuti nella pagina web source. V. il parere n. 1/2008 del Gruppo di lavoro Articolo 29, cit., p. 14.

42. Pertanto, l'editore può tecnicamente inserire nelle proprie pagine web codici di esclusione che limitino l'indicizzazione e l'archiviazione della pagina, rafforzando in tal modo la protezione dei dati personali. Al limite, l'editore potrà ritirare la pagina dal server host, ripubblicarla senza i dati personali in questione ed esigere l'aggiornamento della pagina nelle memorie cache dei motori di ricerca.

43. Di conseguenza, la persona che pubblica il contenuto di una pagina web source è responsabile, in quanto responsabile del trattamento, dei dati personali pubblicati sulla pagina e dispone di diversi mezzi per adempiere i suoi obblighi al riguardo. Questa regolazione della responsabilità giuridica è coerente con i principi consolidati sulla responsabilità dell'editore nell'ambito dei media tradizionali²⁹.

44. Tuttavia, questa responsabilità dell'editore non garantisce che i problemi di protezione dei dati personali possano essere risolti unicamente rivolgendosi ai responsabili del trattamento delle pagine web source. Come sottolineato dal giudice del rinvio, è possibile che gli stessi dati personali siano stati pubblicati su un numero incalcolabile di pagine, cosa che renderebbe difficile, se non impossibile, rintracciare e contattare tutti gli editori interessati. Per di più, l'editore potrebbe risiedere in uno Stato terzo e le pagine web di cui trattasi potrebbero sfuggire all'ambito di applicazione delle norme di diritto dell'Unione relative alla protezione dei dati personali. Potrebbero inoltre sussistere ostacoli giuridici simili a quelli del caso di specie, in cui il mantenimento della pubblicazione originale su Internet è stato considerato legittimo.

45. In realtà, l'accessibilità universale delle informazioni su Internet dipende dai motori di ricerca, dato che trovare informazioni rilevanti senza di essi sarebbe troppo complicato e difficile e produrrebbe risultati limitati. Come osservato giustamente dal giudice del rinvio, ottenere informazioni sugli annunci relativi alla vendita forzata dell'immobile della persona interessata avrebbe richiesto altrimenti una visita agli archivi del giornale. Ora queste informazioni possono essere acquisite inserendo il suo nome in un motore di ricerca su Internet e questo rende la diffusione di tali dati molto più efficiente, ma allo stesso tempo molto più importuna per la persona interessata. I motori di ricerca su Internet possono essere utilizzati per ottenere un profilo completo degli individui tramite la ricerca e la raccolta dei loro dati personali. Orbene, proprio i timori legati alla profilazione degli individui sono stati il motivo che ha ispirato gli sviluppi della moderna legislazione

²⁹ V. sentenza della Corte europea dei diritti dell'uomo, K.U. c. Finlandia, n. 2872/02, §§ 43 e 48, Corte eur. D.U. 2008, nella quale la Corte ha fatto riferimento all'esistenza di obblighi positivi inerenti ad un rispetto effettivo della vita privata e familiare. Questi obblighi possono comprendere l'adozione di misure volte a garantire il rispetto della vita privata anche nell'ambito dei rapporti interpersonali. Nella sentenza K.U. c. Finlandia lo Stato aveva un obbligo positivo di garantire l'esistenza di un rimedio effettivo nei confronti dell'editore.

in materia di protezione dei dati personali³⁰.

46. Per questi motivi è importante esaminare la responsabilità dei fornitori di servizi di motore di ricerca su Internet relativamente ai dati personali pubblicati su pagine web source di terzi accessibili tramite i loro motori di ricerca. In altri termini, nel presente caso la Corte si trova di fronte al problema della «responsabilità secondaria» di questa categoria di prestatori di servizi della società dell'informazione, problema analogo a quello da essa affrontato nelle sue decisioni in materia di marchi e di mercati online³¹.

E – Attività di un fornitore di servizi di motore di ricerca su Internet

47. Un fornitore di servizi di motore di ricerca su Internet può svolgere più tipi di attività. La natura e la valutazione delle suddette attività può variare sotto il profilo della protezione dei dati.

48. Un fornitore di servizi di motore di ricerca su Internet può acquisire in modo automatico dati relativi ai suoi utenti³², vale a dire relativi alle persone che inseriscono termini di ricerca nel motore di ricerca. Questi dati automaticamente trasmessi possono comprendere i loro indirizzi IP, le preferenze (lingua, ecc.) e naturalmente gli stessi termini di ricerca che, in caso di «egosurfing» (ricerche compiute da un utente inserendo il proprio nome), rivelano facilmente l'identità dell'internauta. Inoltre, per quanto riguarda soggetti che hanno un proprio account utente e quindi si sono registrati, i loro dati personali come nome, indirizzo di posta elettronica e numeri di telefono, finiscono quasi invariabilmente nelle mani del fornitore di servizi di motore di ricerca su Internet.

49. A remunerare il fornitore di servizi di motore di ricerca su Internet non sono gli utenti che inseriscono termini nel motore di ricerca, ma gli inserzionisti che acquistano termini di ricerca come parole chiave, in modo che il loro annuncio pubblicitario venga visualizzato contemporaneamente ai risultati delle ricerche di chi utilizza quella parola chiave³³. Ovviamente, i dati personali relativi ai clienti degli inserzionisti entrano in possesso del fornitore di servizi.

³⁰ Internet, tuttavia, non è un'unica e gigantesca banca dati creata dal «Grande Fratello», bensì un sistema decentrato di informazioni che derivano da innumerevoli fonti indipendenti, nel quale l'accesso e la diffusione delle informazioni dipende da servizi di intermediari che, in quanto tali, nulla hanno a che vedere con i contenuti.

³¹ V., al riguardo, le mie conclusioni relative alla sentenza L'Oréal e a., cit., paragrafi 54 e segg.

³² Il che corrisponde alla terza situazione menzionata supra, al paragrafo 3.

³³ Per un esempio di un sistema di pubblicità tramite parole chiave (Google's AdWords) v. le sentenze Google France e Google, cit., punti 22 e 23; del 25 marzo 2010, BergSpechte (C278/08, Racc. p. I2517, punti da 5 a 7); Portakabin, cit., punti da 8 a 10; e Interflora e Interflora British Unit, cit., punti da 9 a 13.

50. La presente domanda pregiudiziale verte tuttavia sull'attività esercitata da Google come semplice fornitore di servizi di motore di ricerca su Internet in relazione a dati, compresi i dati personali, pubblicati su Internet in pagine web source di terzi e trattati e indicizzati dal suo motore di ricerca. Pertanto, i problemi degli utenti e dei clienti degli inserzionisti, ai dati dei quali la direttiva è senza dubbio applicabile con riferimento ai loro rapporti con Google, non hanno rilievo sull'analisi del secondo gruppo di questioni pregiudiziali. Nondimeno, per quanto riguarda i problemi di competenza sollevati dal primo gruppo di questioni pregiudiziali, le suddette categorie di clienti possono essere rilevanti.

V –IL PRIMO GRUPPO DI QUESITI, RELATIVO ALL'AMBITO TERRITORIALE DI APPLICAZIONE DELLA DIRETTIVA

A – Introduzione

51. Il primo gruppo di quesiti pregiudiziali verte sull'interpretazione dell'articolo 4 della direttiva con riferimento ai criteri per stabilire l'ambito territoriale di applicazione della normativa nazionale di trasposizione.

52. Il giudice del rinvio ha suddiviso la questione pregiudiziale relativa all'ambito territoriale di applicazione della normativa spagnola in materia di protezione dei dati in quattro quesiti. Il primo verte sulla nozione di «stabilimento» ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva, mentre il secondo riguarda i casi in cui è fatto «ricorso a strumenti situati nel territorio di detto Stato membro [la Spagna]» ai sensi dell'articolo 4, paragrafo 1, lettera c). Con il terzo quesito il giudice nazionale chiede se sia possibile considerare ricorso a strumenti lo stoccaggio temporaneo delle informazioni indicizzate dai motori di ricerca su Internet e, in caso di soluzione affermativa, se possa ritenersi adempiuto tale criterio di collegamento nel caso in cui l'impresa rifiuti di rivelare il luogo in cui archivia i suddetti indici. Con il quarto quesito si chiede se, alla luce dell'articolo 8 della Carta, debba essere applicata la normativa nazionale di attuazione dello Stato membro in cui si situa il centro di gravità della controversia e nel quale è possibile una tutela più efficace dei diritti dei cittadini dell'Unione europea.

53. Mi occuperò in primo luogo dell'ultimo quesito, che il giudice nazionale ha proposto «a prescindere dalla risposta ai precedenti quesiti, e specialmente nel caso in cui la [Corte] ritenesse inapplicabili i criteri di collegamento previsti all'articolo 4, paragrafo 1, della direttiva».

B – Il centro geografico di gravità della controversia non è di per sé sufficiente a rendere applicabile la direttiva

54. Ai sensi del suo articolo 51, paragrafo 2, la Carta non estende l'ambito di applicazione del diritto dell'Unione al di là delle competenze dell'Unione né introduce competenze nuove o compiti nuovi per l'Unione o modifica le competenze e i compiti definiti nei trattati³⁴. Tale principio si applica anche all'articolo 8 della Carta sulla protezione dei dati personali. Pertanto, l'interpretazione della direttiva conformemente alla Carta non può aggiungere alcun nuovo elemento che faccia scattare l'applicazione territoriale della normativa nazionale di attuazione della direttiva a quelli indicati dall'articolo 4, paragrafo 1, della direttiva stessa. Naturalmente, si deve tener conto dell'articolo 8 della Carta nell'interpretare le nozioni di cui all'articolo 4, paragrafo 1, della direttiva, ma i criteri di collegamento definiti dal legislatore dell'Unione non possono essere integrati da un criterio completamente nuovo attraverso un riferimento al suddetto diritto fondamentale³⁵.

55. Il Gruppo di lavoro Articolo 29 ha giustamente sottolineato che l'ambito di applicazione territoriale della direttiva e della normativa nazionale di attuazione della stessa dipendono o dal luogo di stabilimento del responsabile del trattamento o, quando il responsabile del trattamento sia stabilito al di fuori del SEE, dall'ubicazione dei mezzi e degli strumenti utilizzati. Non sono decisivi la cittadinanza o il luogo di residenza abituale dell'interessato né l'ubicazione fisica dei dati personali³⁶.

56. Il Gruppo di lavoro Articolo 29 ha proposto che nella futura legislazione venga elaborato un approccio orientato ai destinatari del servizio quando i responsabili del trattamento non sono stabiliti nell'Unione³⁷. Nella Proposta della Commissione per un

³⁴ Sentenze del 5 ottobre 2010, *McB*, (C400/10 PPU, Racc. p. I8965, punti 51 e 59); del 15 novembre 2011, *Dereci e a.* (C256/11, non ancora pubblicata nella Raccolta, punti 71 e 72); dell'8 novembre 2012, *Iida* (C40/11, non ancora pubblicata nella Raccolta, punto 78); e del 26 febbraio 2013, *Åkerberg Fransson* (C617/10, non ancora pubblicata nella Raccolta, punto 23).

³⁵ Per esempio, nella sentenza *McB*., la Corte ha respinto un'interpretazione, richiesta sulla base dell'articolo 7 della Carta, del «diritto di affidamento» di cui all'articolo 2, paragrafo 9, del regolamento (CE) n. 2201/2003 del Consiglio, del 27 novembre 2003, relativo alla competenza, al riconoscimento e all'esecuzione delle decisioni in materia matrimoniale e in materia di responsabilità genitoriale, che abroga il regolamento (CE) n. 1347/2000 (GU L 338, pag. 1), che ne avrebbe ampliato il significato. Ciò premesso, naturalmente, una disposizione legislativa dell'Unione che non possa essere interpretata in conformità con i diritti fondamentali tutelati dal diritto dell'Unione dev'essere dichiarata invalida. V. sentenza del 1° marzo 2011, *Association belge des Consommateurs TestAchats e a.* (C236/09, Racc. p. I773, punti da 30 a 34).

³⁶ Gruppo di lavoro Articolo 29, parere n. 8/2010 - WP 179 sul diritto applicabile, pag. 10.

³⁷ Gruppo di lavoro Articolo 29, parere n. 8/2010, pagg. 24 e 31 [p. 36, ndT].

regolamento generale sulla protezione dei dati (2012)³⁸ l'offerta di beni o la prestazione di servizi a interessati residenti nell'Unione europea costituirebbe un fattore di applicazione della normativa dell'Unione in tema di protezione dei dati a responsabili del trattamento stabiliti in paesi terzi. Simile approccio, che collega l'applicabilità territoriale della legislazione UE al pubblico cui ci si rivolge, è coerente con la giurisprudenza della Corte in materia di applicabilità della direttiva 2000/31 sul commercio elettronico³⁹, del regolamento n. 44/2001⁴⁰ e della direttiva 2001/29⁴¹ a situazioni transfrontaliere.

57. Per contro, il criterio del pubblico cui ci si rivolge, nel caso presente gli utenti spagnoli del motore di ricerca su Internet di Google, ai cui occhi la reputazione della persona interessata ha potuto essere compromessa a seguito degli annunci pubblicitari controversi, non appare decisivo per l'applicabilità territoriale della direttiva e della corrispondente normativa nazionale di attuazione.

58. Pertanto, il centro di gravità della controversia in Spagna non può essere aggiunto ai criteri indicati nell'articolo 4, paragrafo 1, della direttiva che, a mio parere, armonizza pienamente la portata territoriale di applicazione delle normative degli Stati membri in materia di protezione dei dati. Ciò vale a prescindere se detto centro di gravità sia costituito dalla cittadinanza o dalla residenza degli interessati, dall'ubicazione dei dati personali controversi nel sito web del giornale o dal fatto che il sito web spagnolo di Google sia diretto specificamente al pubblico spagnolo⁴².

59. Per i suddetti motivi propongo alla Corte, per il caso in cui essa consideri necessario rispondere alla prima questione, di apportare una risposta negativa al quarto quesito.

³⁸ Articolo 3, paragrafo 2, lettera a), della Proposta della Commissione.

³⁹ Sentenza L'Oréal e a. e direttiva n. 2000/31 sul commercio elettronico.

⁴⁰ Regolamento (CE) n. 44/2001 del Consiglio, del 22 dicembre 2000, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU L 12, pag. 1), e sentenze del 7 dicembre 2010, Pammer e Hotel Alpenhof (C585/08 e C144/09, Racc. p. I12527), nonché Wintersteiger, cit. V. inoltre le mie conclusioni relative alla causa Pinckney (C170/12), ancora pendente.

⁴¹ Direttiva 2001/29 del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (GU L 167, p. 10), e sentenza del 21 giugno 2012, Donner (C5/11, non ancora pubblicata nella Raccolta).

⁴² Il rinvio pregiudiziale non specifica cosa si intenda per «centro di gravità», ma la stessa espressione è stata impiegata dall'avvocato generale Cruz Villalón nelle sue conclusioni relative alla sentenza eDate Advertising e Martinez (paragrafi 32 e 55).

C – Applicabilità del criterio dello «stabilimento nell'Unione» al fornitore di servizi di motore di ricerca su Internet di un paese terzo

60. Ai sensi dell'articolo 4, paragrafo 1, della direttiva, il fattore principale che comporta l'applicazione territoriale della normativa nazionale in materia di protezione dei dati è che il trattamento dei dati personali venga effettuato nell'ambito delle attività di uno stabilimento del responsabile del trattamento sito sul territorio dello Stato membro. La legislazione di detto Stato membro si applica, inoltre, nel caso in cui il responsabile del trattamento non sia stabilito nel territorio dell'Unione ma ricorra a mezzi o strumenti⁴³ situati nel territorio dello Stato membro ai fini del trattamento dei dati personali, a meno che detti mezzi o strumenti non vengano impiegati soltanto per il transito sul territorio dell'Unione.

61. Come già sottolineato, la direttiva e il suo articolo 4 sono stati adottati prima che iniziasse la fornitura su larga scala di servizi online su Internet. Inoltre, sotto questo profilo la formulazione letterale non è coerente e completa⁴⁴. Non sorprende che esperti in materia di protezione dei dati personali abbiano avuto difficoltà notevoli nell'interpretarla con riferimento a Internet. I fatti di cui alla presente causa illustrano questi problemi.

62. Google Inc. è una società californiana che possiede controllate in numerosi Stati membri dell'Unione. Le sue attività europee sono, in certa misura, coordinate dalla sua controllata irlandese. Attualmente, essa dispone di centri dati quanto meno in Belgio e in Finlandia. Le informazioni sull'esatta posizione geografica delle funzioni relative al suo motore di ricerca non sono pubbliche. Google sostiene che nessun trattamento di dati personali connesso con il suo motore di ricerca viene effettuato in Spagna. Google Spain agisce in quanto rappresentante commerciale di Google per le sue attività pubblicitarie. In quanto tale, essa ha assunto la responsabilità per il trattamento dei dati personali relativi ai suoi clienti inserzionisti spagnoli. Google nega che il suo motore di ricerca effettui operazioni sui server host delle pagine web source o che raccolga informazioni tramite cookies di utenti non registrati del suo motore di ricerca.

⁴³ Gruppo di lavoro Articolo 29, parere n. 8/2010, p. 10. Il Gruppo di lavoro sottolinea inoltre che il termine «equipment» («strumenti») utilizzato nella versione inglese della direttiva è eccessivamente ristretto, in quanto le altre versioni linguistiche adoperano termini più simili all'inglese «means» («mezzi»), termine che copre anche dispositivi immateriali come i cookies (p. 23 e 24).

⁴⁴ V., in particolare, Gruppo di lavoro Articolo 29, parere n. 8/2010, p. 22, in cui si sostiene che [non l'articolo 4, paragrafo 1, lettera a), bensì] l'articolo 4, paragrafo 1, lettera c), della direttiva dovrebbe applicarsi, malgrado la sua formulazione, quando il responsabile del trattamento ha stabilimenti nell'UE, ma le sue attività sono senza rapporto con il trattamento di dati personali.

63. In questo contesto di fatto, il dettato dell'articolo 4, paragrafo 1, della direttiva non è molto utile. Google possiede numerosi stabilimenti nel territorio dell'Unione. Secondo un'interpretazione letterale, ciò escluderebbe l'applicabilità del criterio riguardante gli strumenti di cui all'articolo 4, paragrafo 1, lettera c), della direttiva. D'altro canto, non è chiaro fino a che punto e dove il trattamento dei dati personali di interessati residenti nell'Unione avvenga nell'ambito delle attività delle sue controllate stabilite nell'Unione.

64. A mio avviso, la Corte dovrebbe affrontare la questione dell'applicabilità territoriale prendendo in considerazione il modello economico dei fornitori di servizi di motore di ricerca su Internet. Come ho indicato, questo modello si basa di solito sulla *pubblicità mediante parole chiave*, che costituisce la fonte del reddito e che, in quanto tale, è la *ragione* per la fornitura di uno strumento gratuito di localizzazione dell'informazione nella forma di un motore di ricerca. L'entità che si occupa della pubblicità mediante parole chiave (denominata nella giurisprudenza della Corte «prestatore di un servizio di posizionamento»⁴⁵) è collegata al motore di ricerca su Internet. Tale entità deve essere presente sui mercati pubblicitari nazionali. Per questo motivo Google ha stabilito controllate in molti Stati membri, le quali chiaramente costituiscono stabilimenti ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva. Google inoltre fornisce domini web nazionali come google.es o google.fi. L'attività del motore di ricerca tiene conto di questa diversificazione nazionale in vari modi nella visualizzazione dei risultati della ricerca, dato che il normale modello di finanziamento della pubblicità tramite parole chiave segue il principio del prezzo per click [payperclick]⁴⁶.

65. Per questi motivi ritengo di dover concordare con le conclusioni del Gruppo di lavoro Articolo 29 secondo le quali dev'essere tenuto in considerazione il modello economico di un fornitore di servizi di motore di ricerca su Internet nel senso che il suo stabilimento ha un ruolo significativo nel trattamento dei dati personali se è collegato ad un servizio implicato nella vendita di pubblicità mirata agli abitanti di tale Stato membro⁴⁷.

66. Inoltre, anche se, per quanto riguarda le sue disposizioni sostanziali, l'articolo 4 della direttiva si basa su un'unica nozione di responsabile del trattamento, ritengo che, per decidere sulla questione preliminare dell'applicabilità territoriale, un operatore economico debba essere considerato come una entità singola e che pertanto, in questa fase dell'analisi, non debba guardarsi alle sue singole attività relative al trattamento di dati personali o ai differenti gruppi di interessati ai quali queste si riferiscono.

⁴⁵ V. sentenza Google France e Google (cit., punto 23).

⁴⁶ V. sentenza Google France e Google (punto 25) e parere n. 1/2008 del Gruppo di lavoro Articolo 29, pp. 5 e 6. È facile verificare che l'uso delle stesse parole chiave su domini nazionali Google diversi può determinare la visualizzazione di risultati e annunci pubblicitari diversi.

⁴⁷ Gruppo di lavoro Articolo 29, parere n. 1/2008, p. 10.

67. In conclusione, il trattamento di dati personali avviene nell'ambito di uno stabilimento del responsabile del trattamento se tale stabilimento funge da collegamento per il servizio di posizionamento per il mercato pubblicitario di tale Stato membro, anche se le operazioni tecniche di trattamento dei dati hanno luogo in altri Stati membri o in paesi terzi.

68. Per questi motivi propongo alla Corte di rispondere al primo gruppo di quesiti pregiudiziali nel senso che il trattamento di dati personali avviene nel contesto delle attività di uno «stabilimento» del responsabile del trattamento, ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva, quando l'impresa che fornisce il motore di ricerca apra in uno Stato membro, ai fini della promozione e della vendita di spazi pubblicitari sul motore di ricerca, un ufficio o una controllata che orienti le proprie attività verso gli abitanti del suddetto Stato.

VI – IL SECONDO GRUPPO DI QUESITI, RELATIVO ALLA PORTATA DI APPLICAZIONE RATIONE MATERIAE DELLA DIRETTIVA

69. Il secondo gruppo di quesiti verte sulla posizione giuridica, alla luce delle disposizioni della direttiva, di un fornitore di servizi di motore di ricerca su Internet che offre accesso ad un motore di ricerca su Internet. Il giudice nazionale ha formulato i suddetti quesiti riferendoli alle nozioni di «trattamento» dei dati personali (quesito 2.1) e di «responsabile del trattamento» (quesito 2.2), alle competenze dell'autorità nazionale per la protezione dei dati di impartire ordini direttamente al fornitore di servizi di motore di ricerca su Internet (quesito 2.3) e all'eventuale esclusione della protezione dei dati personali da parte del fornitore di servizi di motore di ricerca su Internet riguardo ad informazioni legalmente pubblicate da terzi su Internet (quesito 2.4). Gli ultimi due quesiti sono rilevanti solo nel caso in cui si possa considerare che il fornitore di servizi di motore di ricerca su Internet tratta dati personali su pagine web source di terzi ed è il responsabile del loro trattamento.

A – Il trattamento di dati personali ad opera di un motore di ricerca su Internet

70. Il primo quesito del presente gruppo verte sull'applicabilità delle nozioni di «dati personali» e di «trattamento» ad un fornitore di servizi di motore di ricerca su Internet come Google, intendendo per dati personali non quelli di utenti o di inserzionisti, bensì quelli pubblicati su pagine web source di terzi e trattati da un motore di ricerca su Internet gestito dal fornitore di servizi. Nella descrizione del giudice nazionale, il trattamento consiste nel localizzare le informazioni pubblicate o immesse in Internet da terzi, indicizzarle automaticamente, archivarle temporaneamente e infine metterle a disposizione degli utenti di Internet in base ad un particolare ordine di preferenza.

71. A mio avviso, una risposta affermativa al presente quesito non richiede una lunga discussione. La nozione di dati personali viene definita in maniera ampia nella direttiva e tale definizione ampia è stata applicata dal Gruppo di lavoro Articolo 29 e confermata dalla Corte⁴⁸.

72. Per quanto riguarda la nozione di «trattamento», le pagine web source su Internet possono contenere, e spesso contengono, nomi, immagini, indirizzi, numeri di telefono, descrizioni e altre indicazioni per mezzo delle quali una persona fisica può essere identificata. Il fatto che la loro natura di dati personali rimanga «sconosciuta» al fornitore di servizi di motore di ricerca su Internet, il cui motore di ricerca funziona senza intervento umano sui dati raccolti, indicizzati e visualizzati per la ricerca, non modifica questa osservazione⁴⁹. Lo stesso vale per il fatto che la presenza di dati personali nelle pagine web source è in un certo senso casuale per il fornitore di servizi di motore di ricerca su Internet, in quanto per quest'ultimo, o più precisamente per le funzioni di esplorazione, analisi e indicizzazione del motore di ricerca, che riguardano tutte le pagine web accessibili su Internet, può non esserci alcuna differenza tecnica o operativa tra una pagina web source contenente dati personali ed un'altra che non ne contiene⁵⁰. Tuttavia, a mio avviso queste circostanze dovrebbero influire sull'interpretazione della nozione di «responsabile del trattamento».

73. La funzione di esplorazione del motore di ricerca di Google, denominata «googlebot», perlustra Internet in modo costante e sistematico e, procedendo da una pagina web source all'altra sulla base di hyperlink tra le pagine, chiede ai siti visitati di inviarle

⁴⁸ V. articolo 2, lettera a), della direttiva, ai sensi del quale si intende per dati personali «qualsiasi informazione concernente una persona fisica identificata o identificabile». Nel suo parere n. 4/2007, relativo alla nozione di dati personali (WP 136), il Gruppo di lavoro Articolo 29 fornisce un'ampia gamma di esempi. La Corte ha confermato l'interpretazione ampia nella sentenza Lindqvist (cit., punti da 24 a 27). V. anche sentenze Österreichischer Rundfunk e a. (cit., punto 64); Satakunnan Markkinapörssi e Satamedia (cit., punti da 35 a 37); del 16 dicembre 2008, Huber (C524/06, Racc. p. I9705, punto 43); del 7 maggio 2009, Rijkeboer (C553/07, Racc. p. I3889, punto 62); del 19 aprile 2012, Bonnier Audio e a. (C461/10, non ancora pubblicata nella Raccolta, punto 93); e Volker und Markus Schecke e Eifert (cit., punti 23, 55 e 56).

⁴⁹ Il Gruppo di lavoro Articolo 29 ricorda che «non è necessario che le informazioni siano considerate dati personali contenuti in una base dati o in un archivio strutturati. Anche le informazioni contenute sotto forma di testo libero in un documento elettronico possono essere considerate dati personali (...)»; v. parere n. 4/2007, p. 8.

⁵⁰ Esistono motori di ricerca o funzionalità di motori di ricerca che riguardano specificamente i dati personali, i quali possono, in quanto tali, essere identificati per forma (per esempio, i numeri di previdenza sociale) o per composizione (le sequenze di segni corrispondenti a nomi e cognomi). V. Gruppo di lavoro Articolo 29, parere n. 1/2008, p. 14. Tali motori di ricerca possono sollevare problemi particolari in materia di protezione dei dati personali che esulano dall'ambito delle presenti conclusioni.

una copia delle pagine visitate⁵¹. Le copie di queste pagine web source vengono analizzate dalla funzione di indicizzazione di Google. Le sequenze di segni (parole chiave, termini di ricerca) trovate sulle pagine vengono registrate nell'indice del motore di ricerca⁵². Il complesso algoritmo di ricerca di Google valuta inoltre la rilevanza dei risultati della ricerca. Le combinazioni di queste parole chiave con gli indirizzi URL, quando è possibile trovarle, formano l'indice del motore di ricerca. Le ricerche lanciate dagli utenti vengono eseguite all'interno dell'indice. Ai fini dell'indicizzazione e della visualizzazione dei risultati della ricerca, la copia delle pagine viene registrata nella memoria cache del motore di ricerca⁵³.

74. Una copia della pagina web source ricercata, immagazzinata nella memoria cache, può essere visualizzata dopo che l'utente ha effettuato la ricerca. L'utente, tuttavia, può accedere alla pagina originale se, per esempio, vuole visualizzare immagini nella pagina web source. La memoria cache viene aggiornata frequentemente, ma può accadere che la pagina visualizzata dal motore di ricerca non corrisponda più alle pagine web source presenti nel server host a seguito di modifiche o soppressione⁵⁴.

75. Va da sé che le operazioni descritte nei paragrafi precedenti rientrano nel «trattamento» di dati personali sulle pagine web source copiate, indicizzate, immesse nella memoria cache e visualizzate dal motore di ricerca. Più in particolare, tali operazioni comprendono la raccolta, la registrazione, l'organizzazione e la conservazione di questi dati personali e possono comportarne l'impiego, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione e l'interconnessione ai sensi dell'articolo 2, lettera b), della direttiva.

⁵¹ Tuttavia, le cosiddette pagine orfane, che non hanno nessun link ad altre pagine web, rimangono inaccessibili al motore di ricerca.

⁵² Le pagine web trovate dal crawler vengono immagazzinate nella banca dati indicizzata di Google, organizzata alfabeticamente per termini di ricerca, nella quale ciascun invio di indice archivia un elenco di documenti in cui compaiono il termine e la sua posizione all'interno del testo. Alcune parole, come articoli, pronomi e avverbi comuni, nonché alcuni numeri e lettere singole non sono indicizzati. V. http://www.googleguide.com/google_works.html.

⁵³ Queste copie (cosiddette «snapshot») delle pagine web archiviate nella memoria cache di Google consistono soltanto di codici HTML e non di immagini, le quali debbono essere caricate dalla posizione originale. V. Peguera, M., «Copyright Issues Regarding Google Images and Google Cache», *Google and the Law*, pagg. da 169 a 202, in particolare p. 174.

⁵⁴ I fornitori di servizi di motori di ricerca su Internet di solito permettono ai webmaster di chiedere l'aggiornamento della copia della pagina web contenuta nella memoria cache. Le istruzioni relative possono essere reperite sulla pagina «Strumenti per i webmaster» di Google.

B – La nozione di «responsabile del trattamento»

76. Ai sensi dell'articolo 2, lettera d), della direttiva, per «responsabile del trattamento»⁵⁵ si intende «la persona fisica o giuridica (...) che, da sol[a] o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali». A mio avviso, il problema fondamentale nel presente caso è se, e in quale misura, un fornitore di servizi di motore di ricerca su Internet rientri in tale definizione.

77. Tutte le parti, con l'eccezione di Google e del governo ellenico, propongono di dare una risposta affermativa a tale questione, che potrebbe facilmente essere difesa come conclusione logica di un'interpretazione letterale, e forse persino teleologica, della direttiva, dato che le definizioni di base della direttiva sono state formulate in maniera ampia per farvi rientrare i nuovi sviluppi. A mio avviso, tuttavia, un simile approccio rappresenterebbe un metodo che trascura totalmente il fatto che, quando la direttiva è stata redatta, non era possibile prevedere l'emersione di Internet e dei diversi fenomeni connessi.

78. Quando la direttiva è stata adottata, il World Wide Web era una realtà appena comparsa e i motori di ricerca su Internet erano ancora agli inizi. Le disposizioni della direttiva semplicemente non tengono conto del fatto che masse ingenti di documenti e di file elettronici ospitati in maniera decentralizzata sono accessibili da qualsiasi parte del mondo e che i loro contenuti possono essere copiati, analizzati e diffusi da persone che non hanno alcuna relazione con i rispettivi autori o con quanti li hanno caricati in un server host connesso a Internet.

79. Ricordo che nella sentenza Lindqvist la Corte non ha seguito l'approccio massimalista suggerito dalla Commissione riguardo all'interpretazione della nozione di trasferimento di dati verso paesi terzi. La Corte ha dichiarato che, «[t]enuto conto, da una parte, dello stato dello sviluppo di Internet all'epoca dell'elaborazione della [direttiva] e, dall'altra, della mancanza, nel suo capo IV, di criteri applicabili all'uso di Internet, non si può presumere che il legislatore comunitario avesse l'intenzione di includere prospettivamente nella nozione di “trasferimenti verso un paese terzo di dati personali” l'inserimento, da parte di una persona che si trovi nella situazione della [signora] Lindqvist, di dati in una pagina Internet, anche se questi sono così resi accessibili alle persone di paesi terzi in possesso dei mezzi tecnici per consultarli»⁵⁶. Questo implica, a mio parere, che, al fine di ottenere un risultato equilibrato e ragionevole, nell'interpretare la direttiva alla

⁵⁵ Le versioni linguistiche della direttiva [italiana], francese, tedesca, spagnola, svedese e neerlandese parlano di un'entità «responsabile» del trattamento dei dati, la versione inglese parla di un «controller» («controller»), mentre altre versioni, come quella finlandese e polacca, utilizzano termini più neutri (in finlandese «rekisterinpitäjä»; in polacco «administrator danych»).

⁵⁶ Sentenza Lindqvist (cit., punto 68).

luce dei nuovi fenomeni tecnologici debbono essere tenuti in considerazione il principio di proporzionalità, gli obiettivi della direttiva e gli strumenti in essa previsti per il loro raggiungimento.

80. A mio avviso, una questione fondamentale nel presente caso è stabilire se rilevi che, nella definizione del responsabile del trattamento, la direttiva si riferisca al soggetto che «determina le finalità e gli strumenti di trattamento di *dati personali*» (il corsivo è mio). Le parti che considerano Google come responsabile del trattamento fondano questa valutazione sul fatto innegabile che il fornitore di servizi che gestisce un motore di ricerca su Internet determina le finalità e i mezzi del trattamento dati alla luce degli scopi che persegue.

81. Dubito, tuttavia, che una simile analisi porti a un'interpretazione fedele della direttiva quando il trattamento verte su file che combinano dati personali e altri tipi di dati in maniera non sistematica, indiscriminata e aleatoria. Il professore di diritto europeo che ho citato nell'esempio del paragrafo 29 delle presenti conclusioni determina forse le finalità e i mezzi del trattamento dei *dati personali* figuranti nelle sentenze della Corte da lui scaricate sul proprio portatile? L'osservazione del Gruppo di lavoro Articolo 29 secondo cui «[a]nche gli utenti del motore di ricerca potrebbero essere considerati a rigor di termini responsabili del trattamento» rivela l'irrazionalità della cieca interpretazione letterale della direttiva nell'ambito di Internet⁵⁷. La Corte non dovrebbe accogliere un'interpretazione che renda responsabile del trattamento di dati personali pubblicati su Internet virtualmente qualsiasi persona in possesso di uno smartphone o di un tablet o di un computer portatile.

82. A mio avviso, l'economia generale della direttiva, la maggior parte delle sue versioni linguistiche e gli obblighi individuali da essa imposti al responsabile del trattamento si basano sull'idea della *responsabilità del responsabile del trattamento* riguardo ai dati *personali* trattati, nel senso che il *responsabile del trattamento* è consapevole dell'esistenza di una categoria definita di informazioni che corrispondono a dati personali e intende trattare tali informazioni proprio *in quanto* dati personali⁵⁸.

⁵⁷ Gruppo di lavoro Articolo 29, parere n. 1/2008, p. 14, nota 17. Secondo tale parere, il ruolo degli utenti esulerebbe dall'ambito di applicazione della direttiva sulla protezione dei dati in quanto essi esercitano «attività puramente personali». Trovo quest'affermazione non condivisibile. In genere gli utenti di Internet utilizzano motori di ricerca anche per attività che non sono puramente personali, per esempio per fini professionali, di studio, commerciali o nell'ambito del terziario.

⁵⁸ Nel parere n. 4/2007 il Gruppo di lavoro Articolo 29 fornisce numerosi esempi della nozione e del trattamento dei dati personali, responsabile del trattamento compreso, e mi sembra che in tutti gli esempi offerti il suddetto requisito sia soddisfatto.

83. Il Gruppo di lavoro Articolo 29 osserva giustamente che «[i]l concetto di responsabile del trattamento è funzionale, finalizzato cioè all'attribuzione di responsabilità laddove intervenga un'influenza effettiva: si basa quindi su un'analisi fattuale piuttosto che formale»⁵⁹. Il Gruppo prosegue affermando che «il responsabile del trattamento deve determinare quali dati debbano essere trattati per la finalità o le finalità previste»⁶⁰. Le disposizioni sostanziali della direttiva, più in particolare gli articoli 6, 7 e 8, si basano, a mio avviso, sulla premessa che il responsabile del trattamento sappia quel che fa riguardo ai dati personali considerati, nel senso che è consapevole di quale tipo di dati personali sta trattando e perché. In altri termini, il trattamento dei dati deve apparirgli come un trattamento di dati personali, ossia «informazion[i] concernent[i] una persona fisica identificata o identificabile» in una maniera semanticamente rilevante, e non un semplice codice informatico⁶¹.

C – Un fornitore di servizi di motore di ricerca su Internet non è un «responsabile del trattamento» di dati personali su pagine web source di terzi

84. Il fornitore di servizi di motore di ricerca su Internet che offre semplicemente uno strumento di localizzazione delle informazioni non esercita alcun controllo sui dati personali contenuti in pagine web di terzi. Il fornitore di servizi è «consapevole» dell'esistenza di dati personali unicamente nel senso che, sotto un profilo statistico, è probabile che le pagine web contengano dati personali. Durante il trattamento delle pagine web source a scopo di esplorazione, di analisi e di indicizzazione, i dati personali non si manifestano in quanto tali in alcun modo particolare.

85. È questo il motivo per cui considero adeguato l'approccio del Gruppo di lavoro Articolo 29, in quanto esso tenta di tracciare una linea tra le funzioni interamente passive e di intermediazione dei motori di ricerca e le situazioni in cui la loro attività rappresenta un effettivo controllo sui dati personali trattati⁶². Per amor di completezza, occorre aggiungere che stabilire se i dati personali siano divenuti pubblici⁶³ o siano stati legalmente diffusi su pagine web source di terzi non è rilevante ai fini dell'applicazione della direttiva⁶⁴.

⁵⁹ Gruppo di lavoro Articolo 29, parere n. 1/2010, p. 10.

⁶⁰ Ibid., p. 14.

⁶¹ Dammann e Simitis (op. cit., p. 120) osservano che il trattamento con mezzi automatizzati non solo deve riguardare il supporto sul quale i dati sono registrati (Datenträger), ma deve anche riferirsi ai dati nella loro dimensione semantica o sostanziale. A mio parere, è fondamentale che i dati personali siano «informazioni» ai sensi della direttiva, ossia costituiscano un contenuto rilevante sul piano semantico.

⁶² Gruppo di lavoro Articolo 29, parere n. 1/2008, p. 14.

⁶³ Sentenza Lindqvist (cit., punto 27).

⁶⁴ Sentenza Satakunnan Markkinapörssi e Satamedia (cit., punto 37).

86. Il fornitore di servizi di motore di ricerca su Internet non ha alcun rapporto con il contenuto delle pagine web source di terzi su Internet in cui possono comparire dati personali. Inoltre, dato che il motore di ricerca lavora sulla base di copie di pagine web source che il crawler ha estratto e copiato, il fornitore di servizi non ha mezzi per cambiare le informazioni sui server host. Fornire uno strumento di localizzazione di informazioni non implica alcun controllo sul contenuto. Né tale attività mette il fornitore di servizi di motore di ricerca su Internet in condizione di distinguere tra i dati personali ai sensi della direttiva, ossia i dati che si riferiscono ad una persona fisica identificata e identificabile, e gli altri dati.

87. In questa fase, farei leva sul principio enunciato nel considerando 47 della direttiva. In esso si afferma che il responsabile del trattamento di messaggi contenenti dati personali trasmessi tramite telecomunicazioni o posta elettronica è *colui che ha emanato* il messaggio e non la persona che presta i servizi di trasmissione. Questo considerando, così come le deroghe alla responsabilità previste nella direttiva 2000/31 sul commercio elettronico (articoli 12, 13 e 14), si basa sul principio giuridico secondo il quale i rapporti automatizzati, tecnici e passivi relativi ad un contenuto archiviato o trasmesso elettronicamente non implicano alcun controllo o responsabilità sullo stesso.

88. Il Gruppo di lavoro Articolo 29 ha sottolineato che la nozione di responsabile del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati e ad assegnare tale responsabilità a chi esercita un'influenza effettiva⁶⁵. Secondo il Gruppo di lavoro, «[i]l principio di proporzionalità comporta che, nella misura in cui interviene esclusivamente come intermediario, il provider di motori di ricerca non deve essere considerato il responsabile principale del trattamento con riguardo al trattamento di dati personali in questione. In questo caso, i responsabili principali del trattamento sono i fornitori di informazioni»⁶⁶.

89. A mio avviso, il fornitore di servizi di motore di ricerca su Internet non può, né in diritto né in fatto, adempiere gli obblighi del responsabile del trattamento previsti dagli articoli 6, 7 e 8 della direttiva in relazione ai dati personali contenuti in pagine web source ospitate su server di terzi. Pertanto, un'interpretazione ragionevole della direttiva esige che il fornitore di servizi non sia considerato, in generale, rivestire tale posizione⁶⁷.

⁶⁵ Gruppo di lavoro Articolo 29, parere n. 1/2010, pp. 4 e 10.

⁶⁶ Gruppo di lavoro Articolo 29, parere n. 1/2008, pp. 14.

⁶⁷ Tuttavia, il Gruppo di lavoro Articolo 29, nel parere n. 1/2008, p. 14, aggiunge che a stabilire se sussista un obbligo di cancellare o di bloccare i dati personali sono il diritto penale generale e le disposizioni sulla responsabilità vigenti nei singoli Stati membri. In alcuni Stati membri la normativa nazionale prevede procedure di «notifica e rimozione» che il fornitore di servizi di motore di ricerca su Internet deve seguire per non incorrere in responsabilità.

90. Un'opinione contraria implicherebbe che i motori di ricerca su Internet sono incompatibili con il diritto dell'Unione, conclusione secondo me assurda. In particolare, se i fornitori di servizi di motore di ricerca su Internet fossero considerati responsabili del trattamento dei dati personali contenuti su pagine web source di terzi e se in una di queste pagine vi fossero «categorie particolari di dati», ai sensi dell'articolo 8 della direttiva (ossia dati personali che rivelano opinioni politiche e convinzioni religiose o dati relativi alla salute e alla vita sessuale degli individui), l'attività del fornitore di servizi di motore di ricerca su Internet diventerebbe automaticamente illegale, quando le rigorose condizioni dettate nel suddetto articolo per il trattamento di tali dati non siano rispettate.

D – Circostanze in cui il fornitore di servizi di motore di ricerca su Internet è un «responsabile del trattamento»

91. È evidente che il fornitore di servizi di motore di ricerca su Internet controlla l'indice del motore di ricerca che collega le parole chiave agli indirizzi URL pertinenti. Il fornitore di servizi stabilisce il modo in cui l'indice è strutturato e può tecnicamente bloccare alcuni risultati di ricerca, per esempio non mostrando indirizzi URL provenienti da taluni paesi o domini⁶⁸. Inoltre, il fornitore di servizi di motore di ricerca su Internet controlla il proprio indice, nel senso che decide se i codici di esclusione⁶⁹ su pagine web source debbano essere rispettati o meno.

92. Per contro, i contenuti della memoria cache del motore di ricerca su Internet non si possono considerare come rientranti sotto il controllo del fornitore di servizi, in quanto la cache è il risultato di processi totalmente tecnici e automatizzati che producono un'immagine specchio dei dati testuali delle pagine web esplorate, con l'eccezione dei dati esclusi dall'indicizzazione e dall'archiviazione. È interessante che alcuni Stati membri risultano prevedere speciali deroghe orizzontali riguardo alla responsabilità dei motori di ricerca analoghe a quelle previste nella direttiva 2000/31 sul commercio elettronico per alcuni prestatori di servizi della società dell'informazione⁷⁰.

⁶⁸ Vi è chi ha sostenuto che Google effettua un filtraggio di questo tipo in quasi tutti i paesi, per esempio a proposito della violazione di diritti di proprietà intellettuale. Inoltre, negli Stati Uniti sono state filtrate alcune critiche relative a Scientology. In Francia e in Germania Google filtra i risultati di ricerca relativi ad «oggetti di collezione nazisti, ai negazionisti dell'Olocausto, ai sostenitori della supremazia bianca e ai siti che fanno propaganda contro l'ordine costituzionale democratico». Per altri esempi, v. Friedmann, D., «Paradoxes, Google and China: How Censorship can Harm and Intellectual Property can Harness Innovation», *Google and the Law*, pp. da 303 a 327, in particolare p. 307.

⁶⁹ V. supra, paragrafo 41.

⁷⁰ Prima relazione in merito all'applicazione della [direttiva 2000/31 sul commercio elettronico], COM(2003)702 def., p. 13, nota 69, e Gruppo di lavoro Articolo 29, parere n. 1/2008, p. 14, nota 16.

93. Tuttavia, per quanto riguarda i contenuti della memoria cache, a mio avviso la decisione di non rispettare i codici di esclusione⁷¹ su una pagina web implica la responsabilità del provider, ai sensi della direttiva, per il trattamento di tali dati personali. Lo stesso vale nel caso in cui il fornitore di servizi di motore di ricerca su Internet non aggiorni una pagina web nella propria memoria cache nonostante il sito web gliene abbia fatto richiesta.

E – Gli obblighi di un fornitore di servizi di motore di ricerca su Internet in quanto «responsabile del trattamento»

94. È evidente che, se e quando può essere considerato «responsabile del trattamento», il fornitore di servizi di motore di ricerca su Internet è tenuto ad adempiere gli obblighi previsti dalla direttiva.

95. Per quanto riguarda i criteri che rendono legittimo il trattamento dei dati in mancanza del consenso della persona interessata [articolo 7, lettera a), della direttiva], appare evidente che la prestazione di servizi di motori di ricerca su Internet persegue, in quanto tale, interessi legittimi [articolo 7, lettera f), della direttiva], ossia (i) facilitare l'accesso alle informazioni per gli utenti di Internet; (ii) migliorare l'efficacia della diffusione delle informazioni caricate su Internet; e (iii) consentire diversi servizi della società dell'informazione offerti dal fornitore di servizi di motore di ricerca su Internet che sono accessori al motore di ricerca, come l'offerta di pubblicità tramite parole chiave. Questi tre obiettivi si rapportano, rispettivamente, a tre diritti fondamentali tutelati dalla Carta, vale a dire la libertà di informazione e la libertà di espressione (sancite entrambe all'articolo 11) e la libertà d'impresa (articolo 16). Pertanto, un fornitore di servizi di motore di ricerca su Internet persegue interessi legittimi, ai sensi dell'articolo 7, lettera f), della direttiva, quando tratta dati, compresi dati personali, messi a disposizione su Internet.

96. In quanto responsabile del trattamento, un fornitore di servizi di motore di ricerca su Internet è tenuto a soddisfare i requisiti previsti dall'articolo 6 della direttiva. In particolare, i dati personali debbono essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite, ed aggiornati, vale a dire non obsoleti per i fini per i quali sono rilevati. È necessario inoltre ponderare gli interessi del «responsabile del trattamento», o dei terzi a vantaggio dei quali il trattamento viene effettuato, e quelli delle persone considerate.

97. Nel procedimento principale, la persona interessata chiede il ritiro dall'indice di Google dell'indicizzazione del suo nome e del suo cognome assieme agli indirizzi URL delle pagine del giornale in cui sono visualizzati i dati personali che vuole far sopprimere.

⁷¹ V. supra, paragrafo 41.

Infatti, i nomi delle persone vengono utilizzati come termini di ricerca e sono registrati come parole chiave negli indici dei motori di ricerca. Orbene, di solito un nome non è di per sé sufficiente per un'identificazione *diretta* di una persona fisica su Internet, poiché a livello globale esistono molte o addirittura migliaia o milioni di persone che hanno lo stesso nome o la stessa combinazione di uno o più determinati nomi e cognomi⁷². Tuttavia, ritengo che nella maggior parte dei casi la combinazione di un dato nome e cognome come termine di ricerca permetta l'identificazione *indiretta* di una persona fisica ai sensi dell'articolo 2, lettera a), della direttiva, quando i risultati nell'indice di un motore di ricerca rivelano un numero così ristretto di link da consentire ad un utente di Internet di distinguere tra persone che hanno lo stesso nome.

98. Un indice di motore di ricerca collega i nomi e gli altri identificativi che sono utilizzati come termini di ricerca ad uno o più link verso determinate pagine web. Nei limiti in cui il link è adeguato, nel senso che i dati corrispondenti al termine di ricerca compaiono realmente o sono comparsi sulle pagine web linkate, l'indice – a mio avviso – risponde ai criteri di adeguatezza, pertinenza, proporzionalità, esattezza e completezza elencati nell'articolo 6, lettere c) e d), della direttiva. Per quanto riguarda gli aspetti temporali di cui all'articolo 6, lettere d) ed e) (i dati personali debbono essere aggiornati e non debbono essere conservati più a lungo di quanto necessario), occorre esaminare anche questi problemi dal punto di vista del trattamento de quo, ossia la prestazione di un servizio di localizzazione delle informazioni, e non come una questione relativa al contenuto delle pagine web source⁷³.

⁷² La capacità di un nome proprio di identificare una persona fisica dipende dal contesto. Un nome comune può non identificare una persona su Internet, ma sicuramente la identifica, per esempio, all'interno di una classe scolastica. Nel trattamento informatico di dati personali ad una persona viene di solito assegnato un identificativo unico per evitare confusioni tra due soggetti. Esempi tipici di questi identificatori sono i numeri di previdenza sociale. V., al riguardo, Gruppo di lavoro Articolo 29, parere n. 4/2007, p. 13, e parere n. 1/2008, p. 9, nota 11.

⁷³ È interessante sottolineare tuttavia che, nell'ambito dei dati archiviati dalle agenzie governative, la Corte europea dei diritti dell'uomo ha dichiarato che «[i]l diritto interno deve garantire, in particolare, che questi dati siano pertinenti e non eccedenti rispetto alle finalità per le quali vengono archiviati; inoltre, essi debbono essere conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono conservati» (v. sentenza *S. e Marper c. Regno Unito* [GC], nn. 30562/04 e 30566/04, § 103, Corte eur. D.U. 2008; v. altresì sentenza *Segerstedt-Wiberg e a. c. Svezia*, n. 62332/00, § 90, Corte eur. D.U. 2006-VII). Tuttavia, la Corte europea dei diritti dell'uomo ha altresì riconosciuto, nell'ambito dell'articolo 10 della CEDU, relativo alla libertà di espressione, «il contributo essenziale offerto dagli archivi di Internet alla custodia e all'accessibilità di notizie e di informazioni» [v. sentenza *Times Newspapers Ltd c. Regno Unito* (nn. 1 e 2), nn. 3002/03 e 23676/03, § 45, Corte eur. D.U. 2009].

F – Conclusione sul secondo gruppo di quesiti

99. Sulla base di questo ragionamento ritengo che un'autorità nazionale per la protezione dei dati non possa imporre a un fornitore di servizi di motore di ricerca su Internet di ritirare alcune informazioni dal suo indice, salvo i casi in cui tale fornitore di servizi non abbia rispettato i codici di esclusione⁷⁴ o non abbia soddisfatto una richiesta di aggiornamento della memoria cache proveniente dal sito web. Questo scenario non appare rilevante per il presente rinvio pregiudiziale. Un'eventuale procedura di «notifica e rimozione»⁷⁵ relativa a link verso pagine web source a contenuto illecito o inappropriato è una questione di diritto nazionale in materia di responsabilità per danni fondata su motivi diversi dalla protezione dei dati personali⁷⁶.

100. Per i suddetti motivi propongo alla Corte di rispondere al secondo gruppo di quesiti nel senso che, nelle circostanze indicate nella domanda pregiudiziale, un fornitore di servizi di motore di ricerca su Internet «tratta» dati personali ai sensi dell'articolo 2, lettera b), della direttiva. Tuttavia, il fornitore di servizi non può essere considerato «responsabile del trattamento» di tali dati personali ai sensi dell'articolo 2, lettera d), della direttiva, fatta salva l'eccezione sopra illustrata.

VII – LA TERZA QUESTIONE, RELATIVA ALL'EVENTUALE «DIRITTO ALL'OBLIO» DELLA PERSONA INTERESSATA

A – Osservazioni preliminari

101. La terza questione pregiudiziale ha rilevanza solo qualora la Corte respinga la conclusione cui sono pervenuto poc'anzi, secondo la quale, in linea generale, Google non va considerata come «responsabile del trattamento», ai sensi dell'articolo 2, lettera d), della direttiva, oppure convenga con me che in taluni casi a un fornitore di servizi di motore di ricerca su Internet, come Google, può essere riconosciuto un tale status. In ogni altra ipotesi, la sezione che segue è superflua.

102. Ad ogni modo, con la sua terza questione il giudice nazionale chiede se il diritto di ottenere la cancellazione e il congelamento dei dati, previsto all'articolo 12, lettera b), della direttiva, e il diritto di opposizione, previsto all'articolo 14, lettera a), della direttiva, consentano alla persona interessata di contattare essa stessa i fornitori di servizi di motore di ricerca su Internet affinché non indicizzino le informazioni che la riguardano personalmente e che sono state pubblicate su pagine web di terzi. Ciò facendo, l'interessato cerca di impedire che informazioni potenzialmente nocive vengano a conoscenza degli utenti di

⁷⁴ V. supra, paragrafo 41.

⁷⁵ V. articolo 14 della direttiva sul commercio elettronico.

⁷⁶ Gruppo di lavoro Articolo 29, parere n. 1/2008, p. 14.

Internet o esprime il desiderio che le stesse siano dimenticate, anche se sono state pubblicate da terzi legalmente. In altri termini, il giudice nazionale chiede, in sostanza, se dagli articoli 12, lettera b), e 14, lettera a), della direttiva possa essere derivato un «diritto all'oblio». Questo è il primo punto che occorre esaminare nell'analisi qui di seguito esposta, la quale è fondata sul tenore letterale e sugli obiettivi delle summenzionate disposizioni.

103. Se giungerò alla conclusione che gli articoli 12, lettera b), e 14, lettera a), della direttiva, in se stessi e per se stessi, non offrono siffatta protezione, procederò allora a valutare se una simile interpretazione sia compatibile con la Carta⁷⁷. Sarà quindi necessario considerare il diritto alla protezione dei dati personali, di cui all'articolo 8, il diritto al rispetto della vita privata e familiare, sancito all'articolo 7, le libertà di espressione e di informazione, come tutelate dall'articolo 11 (entrambe con riferimento alla libertà di espressione degli editori di pagine web e alla libertà degli utenti di Internet di ottenere informazioni), e la libertà di impresa, prevista all'articolo 16. Infatti, i diritti delle persone interessate previsti agli articoli 7 e 8 debbono essere ponderati con i diritti, garantiti agli articoli 11 e 16, di quanti intendono diffondere i dati o avervi accesso.

B – Se i diritti alla rettifica, alla cancellazione, al congelamento e all'opposizione previsti nella direttiva corrispondano a un «diritto all'oblio» della persona interessata

104. Il diritto alla rettifica, alla cancellazione e al congelamento dei dati previsto all'articolo 12, lettera b), della direttiva, riguarda i dati il cui trattamento non è conforme alle disposizioni della direttiva, *in particolare* a causa della loro incompletezza o inesattezza (il corsivo è mio).

105. Nell'ordinanza di rinvio si riconosce che le informazioni apparse sulle pagine web di cui trattasi non possono essere considerate incomplete o inesatte. Tanto meno si sostiene che siano inesatti o incompleti l'indice di Google o i contenuti della sua memoria cache comprendenti tali dati. Pertanto, il diritto alla rettifica, alla cancellazione o al congelamento, ex articolo 12, lettera b), della direttiva, sorgerà solo nel caso in cui il trattamento da parte di Google dei dati personali provenienti da pagine web source di terzi sia incompatibile con la direttiva per ragioni diverse.

106. Ai sensi dell'articolo 14, lettera a), della direttiva, gli Stati membri debbono garantire alla persona interessata il diritto di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. Ciò vale in particolare nei casi di cui all'articolo 7, lettere e) e f), della direttiva, vale a dire nei casi in cui il trattamento è necessario per un interesse pubblico o per il perseguimento

⁷⁷ Questo è l'approccio seguito dalla Corte nella sentenza McB (cit., punti 44 e 49).

dell'interesse legittimo del responsabile del trattamento oppure di terzi. Inoltre, ai sensi dell'articolo 14, lettera a), «il trattamento effettuato dal responsabile» non può più riguardare i dati controversi in caso di obiezione giustificata.

107. Nei casi in cui i fornitori di servizi di motore di ricerca su Internet sono considerati responsabili del trattamento di dati personali, l'articolo 6, paragrafo 2, della direttiva impone loro di contemperare gli interessi del responsabile del trattamento, o dei terzi a vantaggio dei quali il trattamento viene effettuato, con quelli della persona interessata. Come osservato dalla Corte nella sentenza ASNEF e FECEMD, ai fini di questo contemperamento è rilevante se i dati di cui trattasi figurino già, o meno, in fonti accessibili al pubblico⁷⁸.

108. Tuttavia, come sostenuto da quasi tutte le parti che hanno presentato osservazioni scritte nella presente causa, ritengo che la direttiva non preveda un diritto generale all'oblio nel senso che una persona interessata abbia il diritto di limitare o di porre fine alla diffusione di dati personali che consideri nocivi o contrari ai propri interessi. Sono lo scopo del trattamento e gli interessi da esso tutelati, confrontati con quelli della persona interessata, e non le preferenze di quest'ultima, i criteri da applicare allorché i dati vengono trattati senza il consenso della stessa. Di per sé, una preferenza soggettiva non costituisce un motivo preminente e legittimo ai sensi dell'articolo 14, lettera a), della direttiva.

109. Quand'anche la Corte dovesse dichiarare che i fornitori di servizi di motore di ricerca su Internet sono responsabili in quanto «responsabili del trattamento», quod non, dei dati personali presenti su pagine web source di terzi, la persona interessata non avrebbe comunque un «diritto all'oblio» assoluto da invocare nei loro confronti. Tuttavia, il prestatore di servizi dovrebbe calarsi nella posizione dell'editore della pagina web source e verificare se la diffusione di dati personali sulla pagina web possa, in quel momento, essere considerata legale e legittima ai sensi della direttiva. In altri termini, il fornitore di servizi dovrebbe smettere di mediare tra l'utente e l'editore ed assumere la responsabilità del contenuto della pagina web source e, se necessario, censurarla impedendo o limitando l'accesso alla stessa.

110. Per amore di completezza ricordo che la Proposta della Commissione per un regolamento generale sulla protezione dei dati prevede, all'articolo 17, un diritto all'oblio. Tuttavia, a quanto pare, tale Proposta ha incontrato una notevole opposizione e non è ritenuta costituire una codificazione del diritto vigente, bensì un'importante innovazione

⁷⁸ Sentenza del 24 novembre 2011 (C468/10 e C469/10, non ancora pubblicata nella Raccolta, punti 44 e 45). La Corte europea dei diritti dell'uomo ha sottolineato che la pubblicazione di dati personali in altro luogo pone fine al superiore interesse alla tutela della riservatezza; v. sentenza del 16 dicembre 2010, Aleksey Ovchinnikov c. Russia, n. 24061/04, § 49.

giuridica. Pertanto, essa non sembra influire sulla risposta alla questione pregiudiziale. È tuttavia interessante notare che, ai sensi dell'articolo 17, paragrafo 2, della proposta, «[q]uando ha reso pubblici dati personali, il responsabile del trattamento (...) prende tutte le misure ragionevoli (...) in relazione ai dati della cui pubblicazione è responsabile per informare i terzi che stanno trattando tali dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali». Questa formulazione sembra considerare i fornitori di servizi di motore di ricerca in Internet più come terzi che come responsabili del trattamento in quanto tali.

111. Pertanto, concludo che gli articoli 12, lettera b), e 14, lettera a), della direttiva non prevedono un diritto all'oblio. Mi accingo ora a verificare se questa interpretazione delle suddette disposizioni sia conforme alla Carta.

C – I diritti fondamentali di cui trattasi

112. L'articolo 8 della Carta garantisce a tutti il diritto alla protezione dei dati personali. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

113. A mio avviso, questo diritto fondamentale, costituendo una riaffermazione dell'acquis dell'Unione europea e del Consiglio d'Europa in questo settore, mette in risalto l'importanza della protezione dei dati personali, ma di per sé non aggiunge alcun elemento nuovo all'interpretazione della direttiva.

114. Ai sensi dell'articolo 7 della Carta, ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni. Tale disposizione, sostanzialmente identica all'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950 (in prosieguo: la «CEDU»), dev'essere tenuta in debito conto nell'interpretazione delle disposizioni rilevanti della direttiva, la quale impone agli Stati membri di tutelare *in particolare* il diritto alla riservatezza.

115. Ricordo che anche l'articolo 8 della CEDU copre le questioni relative alla protezione dei dati personali. Per questa ragione, e conformemente all'articolo 52, paragrafo 3, della Carta, la giurisprudenza della Corte europea dei diritti dell'uomo sull'articolo 8 della CEDU è rilevante tanto ai fini dell'interpretazione dell'articolo 7 della Carta quanto ai fini dell'applicazione della direttiva in conformità con l'articolo 8 della Carta.

116. Nella sentenza Niemetz, la Corte europea dei diritti dell'uomo ha concluso che le attività professionali e commerciali di un individuo possono rientrare nell'ambito della vita privata come tutelata dall'articolo 8 della CEDU⁷⁹. Lo stesso orientamento è stato seguito in successive pronunce della Corte.

117. Inoltre, nella sentenza Volker und Markus Schecke e Eifert⁸⁰, la Corte ha dichiarato che «il rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali, riconosciuto dagli [articoli] 7 e 8 della Carta, [è] riferito ad *ogni informazione* [il corsivo è mio] relativa ad una persona fisica identificata o identificabile (...) e (...) che le limitazioni che possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispond[ono] a quelle tollerate nell'ambito dell'[articolo] 8 della CEDU».

118. Sulla base della sentenza Volker und Markus Schecke e Eifert concludo che la protezione della vita privata in base alla Carta, relativamente al trattamento dei dati personali, riguarda tutte le informazioni su un individuo, indipendentemente dal fatto che egli agisca in un ambito del tutto privato o come operatore economico oppure, ad esempio, come politico. Considerata l'ampiezza che nel diritto dell'Unione rivestono le nozioni di dati personali e di trattamento degli stessi, dalla giurisprudenza summenzionata sembra emergere che qualsiasi atto di comunicazione effettuato tramite mezzi automatizzati come telecomunicazioni, posta elettronica o social media che riguardi una persona fisica interferisce potenzialmente con tale diritto fondamentale e necessita pertanto di giustificazione⁸¹.

119. Al paragrafo 75 delle presenti conclusioni ho affermato che un fornitore di servizi di motore di ricerca su Internet effettua un trattamento di dati personali visualizzati su pagine web source di terzi. Inoltre, dalla sentenza della Corte Volker und Markus Schecke e Eifert emerge che, indipendentemente da come vengano qualificate ai sensi della direttiva, le sue attività interferiscono con il diritto alla riservatezza delle persone interessate, sancito all'articolo 7 della Carta. Secondo la CEDU e la Carta, qualsiasi interferenza con i diritti protetti dev'essere basata sulla legge e risultare necessaria in una società democratica. Nella presente causa ci troviamo di fronte non a un'interferenza da parte di autorità pubbliche che necessiti di una giustificazione, bensì al problema di stabilire in che misura

⁷⁹ Corte eur. D.U., sentenze Niemietz c. Germania, del 16 dicembre 1992, serie A n. 251-B, § 29; Amann c. Svizzera [GC], n. 27798/95, *Recueil des arrêts et décisions*, 2000II, § 65; e Rotaru c. Romania [GC], n. 28341/95, *Recueil des arrêts et décisions*, 2000 V, § 43.

⁸⁰ Cit., punto 52.

⁸¹ Per contro, la Corte europea dei diritti dell'uomo si è astenuta dal fornire una definizione del concetto di vita privata in termini positivi. A suo giudizio, quella di vita privata è una nozione ampia, non suscettibile di una definizione esaustiva (v. sentenza CostelloRoberts c. Regno Unito, del 25 marzo 1993, serie A n. 247C, § 36).

possa essere tollerata un'interferenza simile esercitata da privati. I limiti a tale interferenza sono fissati nella direttiva e sono, quindi, basati sulla legge, come richiesto dalla CEDU e dalla Carta. Pertanto, l'interpretazione della direttiva consiste precisamente nell'analizzare alla luce della Carta i limiti al trattamento dati effettuato dai privati. Ne discende la questione di stabilire se esista un obbligo positivo per l'Unione e gli Stati membri di imporre ai fornitori di servizi di motore di ricerca su Internet, che sono soggetti privati, di dare attuazione a un diritto all'oblio⁸². Tale questione ci porta, a sua volta, al problema della giustificazione delle interferenze con gli articoli 7 e 8 della Carta e del rapporto con i concorrenti diritti alla libertà di espressione e di informazione e alla libertà di impresa.

D – Diritti alla libertà di espressione e di informazione e alla libertà di impresa

120. La presente causa riguarda sotto diversi profili la libertà di espressione e di informazione sancita all'articolo 11 della Carta, che corrisponde all'articolo 10 CEDU. Ai sensi dell'articolo 11, paragrafo 1, della Carta, «[o]gni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera»⁸³.

121. Il diritto degli utenti di Internet di cercare e ottenere informazioni messe a disposizione online è tutelato dall'articolo 11 della Carta⁸⁴, il quale riguarda sia le informazioni sulle pagine web source sia le informazioni fornite da motori di ricerca su Internet. Come ho già indicato, Internet ha rivoluzionato l'accesso e la diffusione di ogni tipo di informazione ed ha permesso nuove forme di comunicazione e interazione sociale tra individui. A mio avviso, il diritto fondamentale di informazione merita una particolare protezione nell'Unione, specialmente alla luce della crescente tendenza da parte di regimi autoritari in altre zone del mondo a limitare l'accesso a Internet o a censurare i contenuti

⁸² Riguardo agli obblighi dello Stato di attivarsi per proteggere la vita privata in caso di violazione da parte di privati e alla necessità di temperare ogni intervento in tal senso con il diritto alla libertà di espressione di questi ultimi, v., per esempio, Corte eur. D.U., sentenze *Von Hannover c. Germania*, n. 59320/00, *Recueil des arrêts et décisions* 2004VI, e *Ageyevy c. Russia*, n. 7075/10, del 18 aprile 2013.

⁸³ V. Corte eur. D.U., sentenze *Handyside c. Regno Unito*, del 7 dicembre 1976, serie A n. 24, § 49; *Müller e a. c. Svizzera*, del 24 maggio 1988, serie A n. 133, § 33; *Vogt c. Germania*, del 26 settembre 1995, serie A n. 323, § 52; e *Guja c. Moldavia* [GC], n. 14277/04, § 69, *Recueil des arrêts et décisions* 2008. V. inoltre sentenza del 6 marzo 2001, *Connolly/Commissione* (C274/99 P, Racc. pag. I1611, punto 39), e conclusioni dell'avvocato generale Kokott relative alla sentenza *Satakunnan Markkinapörssi e Satamedia* (cit., paragrafo 38).

⁸⁴ Sentenza del 16 febbraio 2012, *SABAM/Netlog* (C360/10, non ancora pubblicata nella Raccolta, punto 48).

che vi sono immessi⁸⁵.

122. Anche gli editori di pagine web godono di protezione ai sensi dell'articolo 11 della Carta. Rendere un contenuto disponibile online rientra, in quanto tale, nell'ambito dell'esercizio della libertà di espressione⁸⁶, specialmente quando l'editore abbia collegato la propria pagina ad altre pagine e non ne abbia limitato l'indicizzazione o l'archiviazione tramite motori di ricerca, palesando in tal modo la sua volontà di dare ampia diffusione al contenuto. Per gli individui la pubblicazione sul web è un mezzo per partecipare al dibattito o per diffondere la propria opinione o contenuti caricati da altri su Internet⁸⁷.

123. In particolare, la presente domanda pregiudiziale riguarda dati personali pubblicati negli archivi storici di un giornale. Nella sua sentenza *Times Newspapers Ltd c. Regno Unito* (nn. 1 e 2), la Corte europea dei diritti dell'uomo ha rilevato che gli archivi su Internet forniscono un contributo sostanziale alla preservazione e all'accessibilità di notizie e di informazioni: «Tali archivi costituiscono una fonte preziosa per l'insegnamento e le ricerche storiche, specie perché sono immediatamente accessibili al pubblico e generalmente gratuiti. (...) Tuttavia, il margine di discrezionalità di cui gli Stati membri godono nello stabilire un equilibrio tra i diritti in gioco è probabilmente più ampio quando si tratta di informazioni archiviate vertenti su eventi passati che non quando si tratta di informazioni relative ad eventi attuali. In particolare, l'obbligo per la stampa di conformarsi ai principi di un giornalismo responsabile, verificando l'*esattezza* [il corsivo è mio] delle informazioni pubblicate aventi carattere storico, piuttosto che di quelle di attualità, è probabilmente più rigoroso non essendovi l'urgenza di pubblicare il materiale»⁸⁸.

124. I fornitori commerciali di servizi di motore di ricerca su Internet offrono i propri servizi di localizzazione delle informazioni nell'ambito di un'attività economica volta a ricavare proventi dalla pubblicità tramite parole chiave. Questo ne fa un'impresa, la cui libertà è riconosciuta dall'articolo 16 della Carta, conformemente al diritto dell'Unione e al diritto nazionale⁸⁹.

125. Inoltre, occorre ricordare che nessuno dei diritti fondamentali di cui trattasi

⁸⁵ Nazioni Unite, Consiglio dei Diritti Umani, Rapporto del Relatore speciale sulla promozione e la protezione del diritto di libertà di opinione ed espressione, Frank La Rue (Document A/HRC/17/27), del 16 maggio 2011.

⁸⁶ Sentenza *Satakunnan Markkinapörssi e Satamedia* (cit., punto 60).

⁸⁷ Occorre qui ricordare che la deroga per il giornalismo prevista dall'articolo 9 della direttiva si applica «non solo alle imprese operanti nel settore dei media ma anche a chiunque svolga attività giornalistica»; v. sentenza *Satakunnan Markkinapörssi e Satamedia* (cit., punto 58).

⁸⁸ Corte eur. D.U., sentenza *Times Newspapers Ltd* (nn. 1 e 2), § 45.

⁸⁹ Sentenze del 24 novembre 2011, *Scarlet Extended* (C70/10, non ancora pubblicata nella Raccolta, punto 46), e *SABAM/Netlog* (cit., punto 44).

nella presente causa ha carattere assoluto. Tali diritti possono essere limitati, se necessario, alle condizioni stabilite dall'articolo 52, paragrafo 1, della Carta⁹⁰.

E - Se sia possibile derivare un «diritto all'oblio» della persona interessata dall'articolo 7 della Carta

126. Da ultimo, occorre valutare se l'interpretazione degli articoli 12, lettera b), e 14, lettera a), della direttiva alla luce della Carta, e in particolare del suo articolo 7, possa portare a riconoscere un «diritto all'oblio» nel senso indicato dal giudice nazionale. Una constatazione di questo tipo non sarebbe contraria, a priori, all'articolo 51, paragrafo 2, della Carta, in quanto porterebbe a precisare la portata del diritto di opposizione della persona interessata, già riconosciuto dalla direttiva, senza creare nuovi diritti o ampliare l'ambito del diritto dell'Unione.

127. La Corte europea dei diritti dell'uomo ha dichiarato, nella sentenza Aleksey Ovchinnikov⁹¹, che «in alcuni casi può essere giustificato limitare la riproduzione di informazioni già divenute di pubblico dominio, ad esempio al fine di impedire un'ulteriore diffusione dei dettagli della vita privata di una persona estranea a qualsiasi dibattito politico o pubblico su un argomento di importanza generale». Pertanto, in linea di principio, il diritto fondamentale alla protezione della vita privata può essere invocato anche se le informazioni di cui trattasi sono già di pubblico dominio.

128. Tuttavia, il diritto della persona interessata alla protezione della sua vita privata dev'essere contemperato con altri diritti fondamentali, in particolare con la libertà di espressione e la libertà di informazione.

129. La libertà di informazione dell'editore di un giornale tutela il suo diritto di ripubblicare su Internet in via digitale le proprie copie cartacee. A mio parere, le autorità, comprese le autorità per la protezione dei dati, non possono censurare una tale ripubblicazione. La sentenza Times Newspapers Ltd c. Regno Unito (nn. 1 e 2) della Corte euro-

⁹⁰ V. anche sentenza del 18 marzo 2010, Alassini e a. (da C317/08 a C320/08, Racc. p. I2213, punto 63), in cui la Corte ha dichiarato che, «secondo una giurisprudenza costante, i diritti fondamentali non si configurano come prerogative assolute, ma possono soggiacere a restrizioni, a condizione che queste rispondano effettivamente ad obiettivi di interesse generale perseguiti dalla misura di cui trattasi e non costituiscano, rispetto allo scopo perseguito, un intervento sproporzionato ed inaccettabile, tale da ledere la sostanza stessa dei diritti così garantiti (v., in tal senso, sentenza del 15 giugno 2006, Dokter e a., C 28/05, Racc. p. I5431, punto 75, e la giurisprudenza ivi citata, nonché Corte eur. D.U., sentenza Fogarty c. Regno Unito del 21 novembre 2001, *Recueil des arrêts et décisions* 2001XI, § 33)».

⁹¹ Cit., punto 50.

pea dei diritti dell'uomo⁹² dimostra che la responsabilità dell'editore riguardo all'*esattezza* delle pubblicazioni aventi carattere storico può essere più rigorosa di quella prevista per le pubblicazioni di notizie di attualità e può esigere l'uso di apposite *avvertenze che completino* il contenuto controverso. Tuttavia, a mio avviso, nulla può giustificare la richiesta di una nuova pubblicazione, in formato digitale, del numero di un giornale con un contenuto diverso da quello della versione cartacea originariamente edita. Ciò equivarrebbe ad un falso storico.

130. Il problema della protezione dei dati, che è al centro della presente controversia, si pone solo nel caso in cui un utente di Internet inserisca il nome e il cognome della persona interessata nel motore di ricerca ottenendo un link verso le pagine web del giornale in cui compaiono gli annunci contestati. In una situazione di questo genere l'utente di Internet *esercita attivamente il proprio diritto ad ottenere informazioni relative alla persona interessata provenienti da fonti pubbliche* per motivi che solamente lui conosce⁹³.

131. Nella società contemporanea dell'informazione, cercare informazioni pubblicate su Internet tramite motori di ricerca costituisce uno degli strumenti più importanti per esercitare detto diritto fondamentale. Tale diritto comprende, indubbiamente, quello di cercare informazioni relative ad altre persone, ossia, in linea di principio, informazioni protette dal diritto alla vita privata, come quelle che compaiono su Internet a proposito delle attività svolte da un imprenditore o da un politico. Il diritto all'informazione di un utente di Internet sarebbe pregiudicato se la sua ricerca di informazioni su una persona producesse risultati che non riflettono fedelmente le pagine web pertinenti, ma ne offrono solo una versione «bowdlerizzata»⁹⁴.

132. Un fornitore di servizi di motore di ricerca su Internet esercita legalmente tanto la sua libertà di impresa quanto la sua libertà di espressione quando rende disponibili su Internet strumenti di localizzazione delle informazioni sulla base di un motore di ricerca.

133. La costellazione particolarmente complessa e difficile di diritti fondamentali che questo caso presenta osta alla possibilità di rafforzare la posizione giuridica della persona interessata ai sensi della direttiva riconoscendole un diritto all'oblio. Ciò vorrebbe dire sacrificare diritti primari come la libertà di espressione e di informazione. Inoltre, inviterei la Corte a non concludere che questi interessi concorrenti possono essere ponderati in

⁹² Cit. supra.

⁹³ Per quanto riguarda il diritto ad ottenere informazioni, v. sentenze della Corte eur. D.U., *Observer e Guardian c. Regno Unito*, del 26 novembre 1991, serie A, n. 216, § 60, e *Timpul InfoMagazin e Anghel c. Moldova*, del 27 novembre 2007, n. 42864/05, § 34.

⁹⁴ Thomas Bowdler (1754–1825) pubblicò una versione ingentilita dell'opera di William Shakespeare, che voleva essere più adatta a donne e bambini del XIX secolo rispetto a quella originale.

modo soddisfacente in situazioni individuali sulla base di una valutazione caso per caso, lasciando la decisione ai fornitori di servizi di motore di ricerca su Internet. Simili «procedure di notifica e rimozione», se la Corte le richiedesse, porterebbero probabilmente o al ritiro automatico dei link verso qualsiasi contenuto oggetto di un'opposizione oppure ad un numero ingestibile di richieste ai fornitori di servizi di motori di ricerca su Internet più popolari e importanti⁹⁵. In tale contesto, occorre ricordare che le «procedure di notifica e rimozione» di cui alla direttiva 2003/31 sul commercio elettronico si riferiscono a contenuti illeciti, mentre il presente caso verte su una richiesta di soppressione di informazioni legittime e legali entrate nella sfera pubblica.

134. In particolare, i fornitori di servizi di motore di ricerca su Internet non dovrebbero vedersi addossare un simile obbligo. Ciò implicherebbe un'interferenza con la libertà di espressione dell'editore di una pagina web, il quale non godrebbe di una tutela legale adeguata in tale situazione, poiché ogni «procedura di notifica e rimozione» non regolamentata sarebbe una questione privata tra la persona interessata e il fornitore di servizi di motori di ricerca⁹⁶. Questo equivarrebbe ad una censura del contenuto pubblicato effettuata da un privato⁹⁷. È questione del tutto diversa il fatto che gli Stati membri abbiano obblighi positivi di offrire un ricorso effettivo nei confronti dell'editore che violi il diritto alla vita privata, cosa che, nell'ambito di Internet, riguarderebbe l'editore della pagina web.

135. Come osservato dal Gruppo di lavoro Articolo 29, è possibile che la responsabilità sussidiaria dei fornitori di servizi di motore di ricerca su Internet in forza della legislazione nazionale possa implicare obblighi di congelare l'accesso a siti web di terzi aventi contenuti illegali, come pagine web che violano i diritti di proprietà intellettuale o che visualizzano informazioni diffamatorie o criminali⁹⁸.

136. Per contro, nessun diritto generalizzato all'oblio può essere fatto valere nei loro confronti sulla base della direttiva, anche ad interpretarla conformemente alla Carta.

137. Per questi motivi propongo alla Corte di rispondere alla terza questione pregiudiziale nel senso che il diritto di ottenere la cancellazione e il congelamento dei dati, previsto all'articolo 12, lettera b), e il diritto di opposizione, previsto all'articolo 14, lettera d), della direttiva, non comprendono un diritto all'oblio come quello descritto nel rinvio pregiudiziale.

⁹⁵ Sentenza SABAM/Netlog (cit., punti da 45 a 47).

⁹⁶ V. le mie conclusioni nella sentenza L'Oréal e a. (cit., paragrafo 155).

⁹⁷ V. sentenza SABAM/Netlog (cit., punti 48 e 50).

⁹⁸ Gruppo di lavoro Articolo 29, parere n. 1/2008, pp. 14 e 15.

VIII – CONCLUSIONE

138. Alla luce delle suesposte considerazioni, ritengo che la Corte dovrebbe rispondere alle questioni sollevate dall'Audiencia Nacional come segue:

1. Il trattamento dei dati personali viene effettuato nell'ambito delle attività di uno «stabilimento» del responsabile del trattamento, ai sensi dell'articolo 4, paragrafo 1, lettera a), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, allorché l'impresa che fornisce il motore di ricerca crea in uno Stato membro, ai fini della promozione e della vendita di spazi pubblicitari sul motore di ricerca, un ufficio o una controllata che indirizzi le proprie attività verso gli abitanti del suddetto Stato.

2. Un fornitore di servizi di motore di ricerca su Internet, il cui motore di ricerca localizza informazioni pubblicate o immesse in Internet da terzi, le indicizza in modo automatico, le archivia temporaneamente e infine le mette a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, «tratta» dati personali ai sensi dell'articolo 2, lettera b), della direttiva 95/46 quando tali informazioni contengono dati personali.

Tuttavia, il fornitore di servizi di motore di ricerca su Internet non può essere considerato «responsabile del trattamento» di tali dati personali ai sensi dell'articolo 2, lettera d), della direttiva 95/46, fatta eccezione per i contenuti dell'indice del suo motore di ricerca, sempre che il fornitore di servizi non indicizzi o archivi dati personali contro le istruzioni o le richieste dell'editore della pagina web.

3. Il diritto di cancellazione e di congelamento dei dati, previsto all'articolo 12, lettera b), e il diritto di opposizione, previsto all'articolo 14, lettera d), della direttiva 95/46, non consentono alla persona interessata di rivolgersi essa stessa ad un fornitore di servizi di motore di ricerca per impedire l'indicizzazione di informazioni che la riguardano personalmente, pubblicate legalmente su pagine web di terzi, facendo valere la sua volontà che tali informazioni non giungano a conoscenza degli utenti di Internet, quando la persona interessata ritenga che le suddette potrebbero arrecarle pregiudizio o desideri che vengano dimenticate.

Stampato nel mese di aprile 2015
da Tipografia Colitti, Roma - www.tipografiacolitti.it